TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
2,00 €

n.154
www.hackerjournal.it



Il telefono di 007

Abbiamo provato il VERO TELEFONO SPIA

INCHIESTA

ADSL, CHE DISPERAZIONE

perché PAGHIAMO PIÙ
e NAVIGHIAMO PIÙ LENTI

GIOCATTOLI DA SPIA

come TRASFORMARE UN GIOCO
in un ARMA contro la privacy

IL GRANDE BURATTINAIO

Alla scoperta dei SEGRETI DELLE BOTNET


QUATTORD. ANNO 8 - N°154 - 26 GIUGNO / 9 LUGLIO 2008 - € 2,00
9 771594 577001 80154
WLF PUBLISHING

Anno 8 – N.153
26 giugno / 9 luglio 2008

Editore (sede legale):
WLF Publishing S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale



Amarcord di **un Hacker**

"Il progresso ha i suoi svantaggi, di tanto in tanto esplode."
Elias Canetti

Sono passati 25 anni circa da quel fatidico giorno in cui, allora imberbe, vidi il film che cambiò, almeno in parte la mia vita: Wargames di John Badham.

La storia racconta di un ragazzino un po' sfigato, un nerd appassionato di computer che con il suo IMSAI e una modem a 1200 baud si inseriva nel sistema informatico della scuola e cambiava i propri voti, ma non solo, si metteva a giocare con un mega computer della difesa iniziando un gioco che il computer tentava di riportare nella realtà lanciando un attacco nucleare verso il blocco sovietico.

All'epoca avevo a mala pena visto un computer e sicuramente era la prima volta che sentivo parlare di rete informatica, una vera illuminazione, soprattutto per via dei miei voti scolastici che non erano proprio entusiasmanti.

Da allora la tecnologia ha fatto passi da gigante e molti di voi non hanno mai utilizzato un modem a 56k e non sanno cosa sia un floppy disk (installare un programma come Photoshop significava prendersi una mezza giornata e 6/7 floppy da infilare uno dietro l'altro) però mi piacerebbe che i più giovani tra i voi lettori vedessero quel film e provassero lo stupore che ho provato io, e molti come me, nel capire quanto si stava rivoluzionando il mondo, una rivoluzione che è ancora in corso con il social networking (ormai termine stra-abusato) e con tutte le forma di interazione tra persone a cavallo della rete.

Un'altra considerazione vorrei fare... era il 1983 e sto "fetente" viveva in un posto dove la scuola era già in rete... da noi alcune scuole, molte, non lo sono ancora adesso... malgrado la tecnologia sia ora meno costosa e più accessibile, lui lavorava in Dos e stringhe di comando, e io mi chiedo per quanti anni ancora dovremo subire questo gap con gli altri paesi "evoluti", per quanto tempo saremo il fanalino di coda europeo per la percentuale di penetrazione dell'uso del computer...

Comunque non vorrei perdere la dolcezza dei miei ricordi in polemiche che abbiamo già fatto e visto, vi prego solo di ricordare cosa c'è stato prima di noi e apprezzare la fortuna che abbiamo di vivere in questo tempo così come di riconoscere gli errori che abbiamo fatto e cercare di correggerli per chi verrà dopo di noi.

BigG

CONTINUA LA CACCIA

In tanti ci hanno già risposto ma non ci basta mai e vogliamo solo il meglio per le nostre pagine e i nostri lettori e quindi continuate a mandare le vostre candidature alla mail:

contributors@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Deutschland, Deutschland UBER ALLES

Germania, germania, sopra tutti, sicuramente non nella difesa della privacy

Non so quanti abbiano sentito parlare di una normativa applicata in Germania da circa sei mesi e che risponde al nome di Data Retention. In pratica di si tratta dell'obbligo nei confronti dei gestori di telefonia e di linee internet di mantenere i dati riguardanti le comunicazioni dei propri utenti per un certo periodo di tempo.

Un recente studio ha dimostrato che l'applicazione di questa normativa ha portato la popolazione tedesca a utilizzare meno la rete e il telefono personale per le proprie comunicazioni dimostrando che questo tipo di norma, estremamente invasiva della privacy non può che portare ad un'involuzione del mercato e della società.

L'11% degli intervistati ha dichiarato di aver rinunciato all'uso del telefono o della mail per le proprie comunicazioni personali e, cosa ben più significativa, il 52% ha dichiarato che qualora avesse bisogno di ricorrere alle cure di uno psichiatra o di un centro aiuto contro le dipendenze (alcol o droga) esiterebbe ad utilizzare il telefono per contattarli onde evitare di lasciare traccia di questi problemi per i successivi mesi.





Ricordiamo a tutti che un'analoga norma vige anche in Italia per quanto riguarda la telefonia, i gestori sono difatti a costretti a mantenere traccia di chi abbiamo chiamato, quando e per quanto tempo per 6 mesi mentre la legge non si pronuncia per quanto riguarda il contenuto delle comunicazioni che non dovrebbe quindi essere conservato.

Come se non bastasse, sempre in Germania, è stata fatta una proposta che permetterebbe alla Polizia di immettere in rete dei "trojan autorizzati" per poter spiare i sospetti. Il ridicolo è che la polizia dovrà utilizzare sistemi analoghi a quelli dei pirati informatici, mail contenenti malware, sperando che gli indagati siano così sconsiderati da aprirle e da farsi infettare. Quello che da un po' da riflettere è che la Corte Suprema Federale tedesca si è appena dichiarata contro una legge analoga e ha dichiarato illegale lo spionaggio da parte della polizia verso privati cittadini, non si capisce quindi come possa passare questa nuova proposta. ■



OFFICE 2007 GRATIS!

Non abbiamo comprato l'ultima versione di Office 2007 ma ci farebbe tanto comodo averne una? Non c'è problema! In internet si posso trovare centinaia di video dove spiegano, passo passo, tutte le procedure per ottenere, da una demo, una versione full a tuttti gli effetti. Forse, non sarà legale ma la procedura è molto semplice: basta scaricare una demo del software dal sito di Microsoft e con un paio di passaggi si ottiene la versione completa. Certo, Microsoft Italia dichiara che le versioni originali sono molto più complete e hanno la possibilità di aggiornarsi ma per chi ne fa basilari usi domestici la versione pirata può andare più che bene.

APPLE SOTTO TIRO

Se è vero che gli utenti Apple sono notoriamente privilegiati nel non venire attaccati da virus o phishers per il semplice fatto che i prodotti Mac sono prodotti di nicchia è pur vero che da qualche tempo, la nota casa americana, sta ampliando il suo piazamento sul mercato, prima con iPode poi con iPhone e con le nuovissime versioni economiche di portatili MacBook. Questo sta portando a spostare il mirino di alcuni sviluppatori di virus che negli ultimi mesi hanno preso d'assalto gli utenti che usano iTunes Store. La sola consiste, come al solito, nel dirigere l'utente, tramite una mail, ad un indirizzo web fasulo fotocopia del famoso store Apple. Una volta arrivati a questa pagina si è fregati. Il computer si impalla e nel giro di pochi secondi vengono ispezioni tutti gli angoli del nostro hard-disk alla ricerca di informazioni sensibili. Il consiglio è sempre lo stesso signori. Occhi ben aperti e leggiamo gli indirizzi prima di cliccarli.



UN PROIETTORE NEL PORTATILE

Tutti noi ci domandiamo quale sia la prossima integrazione che verrà fatta sui nostri laptop. Un'anteprima di risposta è stata data al Computex 2008 di Taipei dove, a grande stupore, è stato presentato l'ultimo modello Asus G1S con proiettore integrato.Si tratta di un vero e proprio proiettore orientabile che è posizionato dove oggi, nei modelli più recenti, troviamo la webcam.



Il nuovo assemblamento permette di proiettare immagini in alta risoluzioni a colori, non comporta altre alimentazioni specifiche.

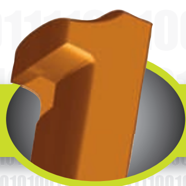
Diciamo che sarebbe il massimo per chi è abituato a vedersi i film su un 15 pollici.

Aspettiamo fiduciosi altri sviluppi.

IN GALERA I SITI PORNO

Sappiamo tutti che la rete è satura di siti pornografici o di punti di incontro telematici dove incontrare donnine che si spogliano davanti alla webcam a pagamento. Ed è per questo che la parlamentare israeliana, Zahava Gal-O, richiede una legge ove si possano prevedere fino a cinque






HOT NEWS

L'ADDIO DI BILL

È ormai cosa nota che il nostro amato "Zio Bill" sta lasciando l'immagine di icona di Microsoft, per ritirarsi a dolce vita di pensionato ultramiliardario. Ma non perde occasione per portare al suo ultimo TechEd, di Orlando, le due nuovissime anteprime su Silverlight 2 e Explorer 8 i quali faranno la loro prima comparsa tra un paio di settimane in negozi di informatica. Mentre per IE 8 Beta 2 bisognerà aspettare intorno ad ottobre 2008 perché le finiture del software stanno richiedendo maggiori attenzioni agli sviluppatori. Ed è proprio a questultimi che Gates lascia un particolar saluto dicendo: "ho iniziato come uno sviluppatore e sviluppatore rimango nel cuore".

CONCORSO LINUX

L'associazione Linuxtrent ha indetto un concorso giornalistico aperto a tutti. Se avete scritto in italiano un articolo sull'etica del software libero e l'avete pubblicato su un quotidiano o periodico cartaceo o digitale, preferibilmente con sede nelle regioni dell'arco alpino, leggete il regolamento e inviate i vostri lavori: verranno letti e valutati da una giuria. La comunicazione al pubblico non specialistico è una delle eterne palle al piede di Linux e del software libero in generale: è difficile che attecchisca se non c'è nessuno che spieghi in termini semplici e pratici quali sono i suoi vantaggi per l'utente comune. Il vostro lavoro potrebbe contribuire a colmare questa lacuna. Che ne dite?

SPIATI LO STOMACO

Un fantastico progetto nato dalla collaborazione tra Given Imaging, l'ospedale israeliano di Amburgo e il Royal Imperial College di Londra ha portato alla nascita di una "telecamera-pillola" in grado di entrare nel nostro stomaco e aiutare i medici a diagnosticare mali che prima venivano visualizzati dalle radiografie o risonanze, che alla lunga danneggiano il nostro corpo. La PillCam è biocompatibile e la sua grande innovazione è quella di poterla governare all'interno del nostro corpo come fosse un mouse. La cosa più curiosa quanto inquietante è che per fermare la pillola o muoverla bisogna manovrerla con un magnete al di fuori del nostro corpo. Il dottor Frank Volke non è affatto preoccupato e rassicura tutti gli investitori che l'apparecchio non ha nessun punto debole. Speriamo bene.

ARRIVA L'ODF DI OFFICE

Lo scorso 21 maggio, Microsoft ha dichiarato che il Service Pack 2 di Microsoft Office 2007, in uscita per la prima metà del 2009, supporterà l'attesissimo il formato ODF (OpenDocument), lo standard ISO 26300 utilizzato da vari programmi alternativi alla suite Microsoft, come OpenOffice.org. L'utente sarà in grado di aprire, modificare e salvare documenti usando ODF e in oltre avranno la possibilità di impostare l'ODF come formato di file di default per Office. Microsoft ha osservato molto attentamente le richieste su questa specifica estensione perché è l'unica a essere in grado di farsi gestire da programmi diversi tra loro cancellando il fastidioso vincolo che si ha quando creiamo un file con un programma e dobbiamo darlo a persone o società che non lo supportano.



anni di carcere per coloro che compilano i contenuti o che si occupano di curarne la grafica delle suddete "case a luci rosse" telematiche.
La prostituzione in Israele è proibita in ogni ambiente: dalle abitazioni ai locali, dalle automobili ai veicoli marittimi. Galon, nella proposta redatta sotto la sua supervisione, chiede al parlamento di aggiungere alla lista dei luoghi anche i siti web, perché non vengano considerati un'eccezione, perché sia chiaro a tutti che la prostituzione non è un reato tollerato in nessuna della sue forme.

GMAIL COL BUCO

Il noto gruppo di ricerca sulla sicurezza informatic, Insert, dichiara nel suo ultimo comunicato stampa che il sistema di gestione di Gmail, servizio di posta elettronica on-line di Google, ha un buco che se violato da la possibilità di disseminare migliaia e migliaia di spam. Il problema starebbe nella mal gestione del forwarding e dei provider di Gmail che sono facilmente accessibili tramite SMTP e HTTP diventando così open relay. Insert, in fase dimostrativa, è riuscita a mandare ben 4000 messaggi di spam da un singolo account Gmail senza che vi fosse alcun intervento da parte di Google. La suddetta agenzia non ha pubblicato apertamente i dettagli della falla, ma li ha comunicati ai legittimi proprietari dell'errore. Una volta risolto il problema, hanno dichiarato, pubblicheremo i resoconti ad una conferenza sulla sicurezza informatica che si terrà in settembre in Brasile.



SECOND LIFE

Second Life, il mondo virtuale che ha impazzato tra i suoi miglioni di utenti, ha acquisito un utente molto particolare che apre le morte della bioscenza informatica. Stiamo parlando di un giovane americano, che è rimasto paralizzato in un brutto incidendente che lo ha condannato, da ormai trentanni, alla paralisi semi-totale. Il giovane, che vuole mantenere l'anonimato, è stato aiutato da un ecipe medica che ha studiato il modo di far muovere un avatar con la forza del pensiero. Infatti, grazie al posizionamento di tre elettrodi sulla testa del paziente si possono monitorare le sue onde celebrali le quali vengono inviate ad un PC che poi le trasforma in movimento. E così dopo trentanni il nostro giovane amico ha potuto rivedere muovere il proprio corpo, anche se solo virtuale, grazie alla forza dell'unica parte di se che non ha mai cessato di muoversi. Il suo cervello.

PHISHING IN UN FLASH

C'è una falla nel Flash Player di Adobe che ancora non dispone di una patch e che pare stia diventando sempre più diffusa. Lo scopo, naturalmente, è riuscire a eseguire codice arbitrario sulla macchina della vittima.

La situazione è ulteriormente complicata dal fatto che circa 20.000 pagine web sono stato contaminate con del codice che redirige i browser verso i siti che ospitano animazioni Flash create per sfruttare la falla del player.



Flash è installato praticamente su ogni computer al mondo: ne esistono versioni per Windows, Linux e MacOs X. Pertanto, la vulnerabilità è da ritenersi estremamente seria.

Il team per la sicurezza di Adobe sta lavorando insieme a Symantec per raccogliere abbastanza informazioni da poter rilasciare un aggiornamento.

LUNGA VITA A XP

In occasione del Computex che in questi giorni si sta tenendo a Taipei (Taiwan), Microsoft ha confermato di nuovo quanto già si sapeva: Windows Xp potrà essere installato fino al 2010 sui Pc a basso costo.

D'altra parte, se vuole conquistare una fetta di questo particolare settore, Microsoft non può certo affidarsi a Windows Vista, affamato di risorse com'è. L'unica vera novità riguarda l'adozione ufficiale della definizione di net-top per quei portatili dall'hardware minimale ideati unicamente per consentire la navigazione in Internet e la consultazione della posta elettronica: all'esistenza di queste macchine in particolare si deve la decisione di prolungare la vita di Windows Xp.



CHRISTINE PER IL P2P

Dopo i diritti per la cosiddetta copia privata, nel mirino del massimo organo di controllo amministrativo francese c'è ora la legge comunemente detta "Internet e creatività", a suo tempo voluta dall'HADOPI.

A detta di Christine Albanel, attuale ministro per la cultura, la legge non sarà esaminata prime dell'estate, quindi ci sarebbe tutto il tempo per le eventuali modifiche; infatti il Consiglio di Stato ha emesso un avviso di "presa in esame" in relazione a diversi punti e pare assai lontano dall'approvazione della "legge internet e creatività". Noi naturalmente tifiamo Christine per l'inizio dell'estate.



LA VOLPE PORTA GUAI

Nel mese di giugno l'attesa versione 3 di Firefox farà il suo debutto, ma sulla nascita si vanno addensando nubi oscure.

Infatti sono stati identificati due bug nella Release Candidate 1 del browser; alcuni di una serietà tale che stanno facendo considerare la possibilità di rilasciare una Rc2 finora non prevista prima della versione definitiva.

In particolare, i problemi peggiori si



HOT NEWS

IL MICROSCOPIO SUL CELLULARE

Non necessita di installazioni troppo complicate, basta pluggare il CellScope in modo tale che il cellulare sia allineato esattamente all'altezza delle lenti aggiuntive, in corrispondenza dell'obiettivo integrato. Un team di ricercatori dell'Università di Berkeley ha sviluppato e sta perfezionando una tecnologia che può permettere a qualsiasi persona di riconoscere la malaria semplicemente utilizzando questo microscopio, anche senza aver studiato alcunchè di medicina.



Sarà l'inizio di una nuova schiera di medici senza frontiere?



FOGLIE A ENERGIA SOLARE

Un nuovo componente impredibile per la casa hitech: una pianta che si posiziona sul davanzale e che fa il pieno di energia solare, grazie ai pannelli a forma di foglia, archiviandola nella batteria interna al litio che poi può trasferire il succo vitale a tutti i device tecnologici come cellulari, fotocamere, navigatori satellitari, ecc...



Si tratta di una creazione del Japan's National Institute, in collaborazione con Mitsubishi Corporation e Tokki Corporation ed è stata recentemente presentata alla stampa come un prototipo in grado di mimetizzarsi perfettamente in casa e che aprirà la via a altri pannelli che si potranno includere in muri e tappezzeria visto che si può contare su una nuova generazione di superfici sottili e efficenti.

PUMA CONTRO CENTRINO

Amd ha registrato perdite nei bilanci per il sesto trimestre di fila; Amd ha perso significative quote di mercato a favore di Intel; nonostante tutto questo, Amd non si arrende.

Il ritardo con cui la piattaforma Centrino 2 di Intel arriverà sul mercato è l'occasione per il riscatto, e il mezzo per ottenerlo è rappresentato dai processori Griffin e dalla piattaforma Puma, presentati al Computex 2008.

Tutta la piattaforma Puma è dunque progettata per ottimizzare l'esperienza mobile, con una particolare attenzione alla durata della batteria: l'integrazione tra i vari componenti è state ideata tenendo presente questa esigenza degli utenti, che in numero sempre maggiore scelgono di dotarsi di un laptop anziché di un desktop.

riscontrano nell'edizione per Linux di Firefox: due bug esclusivi per il sistema operativo del pinguino sono la spiegazione per i rallentamenti e i blocchi dell'applicazione segnalati da molti utenti.

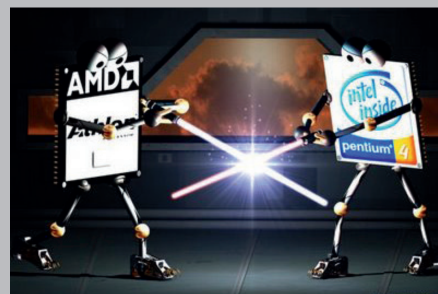
Un browser che di tanto in tanto occupa la Cpu al 100 per cento e deve essere terminato affinché l'utente possa tornare a usare il Pc è intollerabile, ma alla Mozilla Foundation, in realtà, non sembrano prendere troppo sul serio la situazione. Staremo a vedere.



INTEL FA LA FURBA

Intel è stata multata in Corea del Sud per aver violato le norme antitrust: il comportamento sanzionato riguarda un'offerta di sconti cha ha spinto gli utenti a preferire i prodotti marchiati Intel rispetto a quelli di Amd.

Per questo la Fair Trade Commission coreana ha comminato una sanzione pari a 25 milioni di dollari. I guai per la compagnia di Santa Clara, tuttavia, non finiscono qui: la Commissione Europea sta indagando per scoprire se Intel si sia macchiata di concorrenza sleale nel mercato europeo, mentre negli Stati Uniti la rivale Amd l'ha denunciata per lo stesso motivo.

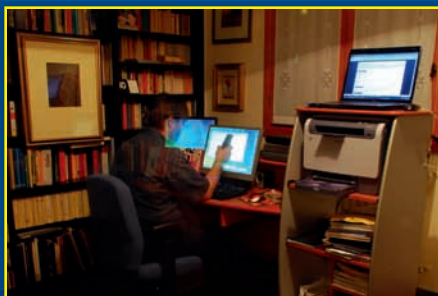


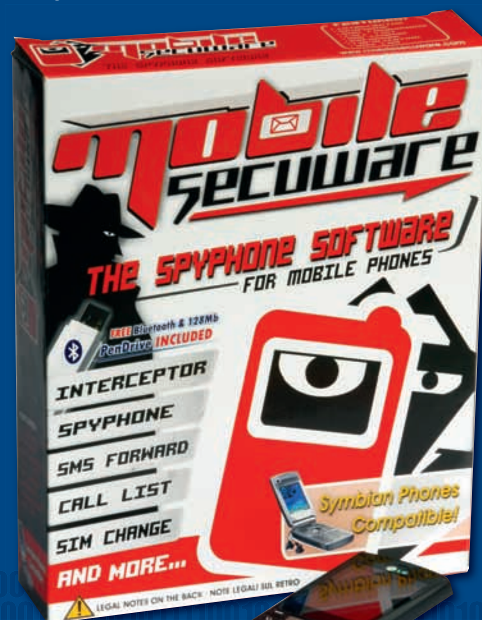
Il telefono che SPIA



È identico in tutto a un normale telefono Nokia N95, ma grazie a uno speciale software è possibile spiare chi lo usa. Hacker Journal l'ha provato per voi

Qualche mese fa la Guardia di Finanza ha denunciato 420 persone che avevano modificato un telefono cellulare in modo che potesse spiare fidanzate, mariti, dipendenti e amanti, usando uno speciale software. Scoprendo, tra l'altro, che in un palazzo nella periferia di Napoli viveva una coppia in cui il marito era l'amante di una donna dello stesso palazzo. Niente di strano, se non il fatto che il marito di quest'ultima era l'amante proprio della donna il cui marito gli metteva le corna con sua moglie. Complicato? Lo è stato molto di più quando la solita Guardia di Finanza ha scoperto che i quattro, evidentemente sospettosi, si controllavano a vicenda tramite telefoni spia. Probabilmente uno di quelli che Hacker Journal ha messo alla prova. Ce l'ha gentilmente mandato la società NeoCall, che li vende online senza problemi e legalmente (anche perché ha la sede legale a San Marino) all'indirizzo www.neocall.it. Se vendere telefoni spia da San Marino è legale, così come non è un reato in sé comperarli, usarli per controllare persone a loro insaputa è però decisamente illegale. La legge 98 del 1974 recita testualmente: "Chiunque, fraudolentemente prende cognizione di una comunicazione o di una conversazione, telefoniche o telegrafiche, tra altre persone o comunque a lui non dirette, ovvero le interrompe o le impedisce è punito con la reclusione da sei mesi a quattro anni". Ed è proprio quello che possono fare questi telefoni, che possono essere di qualsiasi marca e modello purché basati su Symbian e dotati di un software che non ha rivali in fatto di spionaggio telefonico.









Naturalmente se si dichiara di acquistarli per usi leciti, non si compie reato. Anche se gli usi leciti sono un po' noiosi: controllo dei neonati, localizzare animali domestici, monitoraggio di rumori naturali, usi sperimentali e didattici nel campo dell'alta frequenza e così via.



:: Cavia avvisata mezza salvata

Chi vuole un telefono spia che faccia tutto può comperare da NeoCall il Nokia N95 con la Neo-Suite 2K8 OS9 e Neo-Gps. Il prezzo è un po' alto, 1.399 euro, ma chi vuole solo la Neo-Suite se la cava con 499 euro. Si possono comperare anche solo qualche modulo: quello per intercettare gli Sms costa dai 120 ai 195 euro, a seconda del sistema operativo Symbian. Noi che vogliamo tutto o niente abbiamo provato proprio il Nokia N95 con la Neo-Suite 2K8 OS9 e Neo-Gps. Lo abbiamo dato a una "cavia", avvisata del fatto che era un telefono spia e che non parlasse eccessivamente male di noi durante, che ci ha inserito la sua Sim e se l'è portato in ufficio. Bene, dalla nostra redazione a metà mattina abbiamo cominciato ad agire. Per sgranchirci le dita e le orecchie abbiamo chiamato il telefono spia dal nostro telefono "pilota", un cellulare normale che però è stato impostato nella configurazione iniziale in modo che il Nokia della cavia lo riconosce e accetti comandi molto particolari. Il telefono spia ha riconosciuto la nostra chiamata e ha aperto automaticamente la conversazione.



Senza vibrare, senza che si accendesse una luce, senza squillare. Senza dare segni di vita, insomma. Ma consentendoci di ascoltare tutte le conversazioni nel raggio di azione del microfono del telefonino. Al primo tentativo, per la verità, non ci è andata molto bene visto che la cavia era donna e da brava donna lo teneva nella borsetta. Un po' si sentiva, ma confusamente. Mezz'ora dopo l'audio era chiarissimo. Evidentemente lo aveva appoggiato sulla scrivania.



:: Spiare a fondo

Dopo aver rotto il ghiaccio ascoltando qualche pettegolezzo da ufficio, abbiamo inviato al telefono spia il comando, via Sms, che consente di intercettare gli Sms della nostra cavia. Ogni volta che ne riceveva o ne spediva uno, arrivavano anche sul



nostro telefonino. Utile. Anzi, utilissimo, visto che una recente indagine inglese ha stabilito che la maggior parte dei fedifraghi manda messaggini teneri o osè e il partner li scopre mandando a rotoli il matrimonio. Inviamo un altro codice via Sms (naturalmente il telefono spia non li evidenzia e non compaiono tra gli altri Sms) per ricevere una notifica via Sms con ogni numero delle chiamate che la nostra amica fa e riceve. Se la nostra fidanzata chiama 18 volte lo stesso numero nell'arco della giornata, e quel numero non è né il nostro ne quello della sua mamma, allora forse l'investimento nel telefono spia aveva un suo perché. In teoria avremmo potuto anche ascoltare le sue telefonate, ma la sua Sim avrebbe dovuto essere abilitata alla conferenza (chiamate a tre). E non lo era. Infine, con procedura un po' più laboriosa, abbiamo attivato la funzione del software Neo-Gps (199 euro, se si compera a parte) che consente di vedere in quale cella si trova il cellulare spia, e quindi stabilirne la posizione con una certa precisione. Niente da dire, un software molto interessante. Peccato che non sia per niente legale usarlo per spiare le persone.

Moreno Soppelsa





I giocattoli spia preoccupano i servizi segreti

Crediamo che i giocattoli del nostro fratellino siano inoffensivi? Come il numero uno della casa automobilistica Porsche, rischiamo di dover cambiare idea. Oggigiorno, i giocattoli possono trasformarsi in accessori degni di 007... e non solo al cinema

Non ci sono dubbi: James Bond deve guardarsi le spalle. I dispositivi in grado di svolgere efficaci attività di spionaggio sono sempre più numerosi. Strumenti atti ad ascoltare, vedere e sorvegliare possono nascondersi negli oggetti più impensati. Dopo il rischio di essere ascoltati attraverso il pupazzo Furby e lo spionaggio tramite webcam, entra in scena la sorveglianza pirata tramite babyphone. I genitori conoscono bene questi piccoli strumenti che consentono di ascoltare a distanza il bambino che dorme nella sua cameretta. Il proprietario della casa automobilistica Porsche non immaginava certo di essere a sua volta ascoltato tramite un babyphone. In aprile, il settimanale tedesco Der Spiegel ha riportato che Wendelin Wiedeking, il boss di Porsche, era stato spiato in un albergo di lusso, il Ritz-Carlton di Wolfsburg. Il dispositivo era semplicemente nascosto sotto la sua poltrona. Queste attività di spionaggio hanno colpito anche altri dipendenti dell'azienda. Il responsabile del consiglio d'amministrazione si è trovato il cellulare intercettato. Un ex-dirigente di Volkswagen si è invece ritrovato un dispositivo di ascolto nascosto nell'appartamento. Insomma, l'acquisto di Volkswagen da parte della casa produttrice di auto di lusso Porsche sembra interessare a molti.

::Provati dalla redazione

In redazione abbiamo esaminato alcuni dispositivi che possono essere trasformati in strumenti di spionaggio. Non costano centinaia di euro e non si tratta nemmeno di gadget militari. Per procurarceli abbiamo adottato un approccio molto semplice. Siamo andati in qualche negozio di giocattoli e abbiamo provato alcuni oggetti che potrebbero essere usati per violare la nostra sicurezza.

Il detector Spy Micro Tracker System permette ai bambini di sorvegliare tutti i movimenti che hanno luogo all'interno di un'abitazione. Il giocattolo ha una portata di 25 metri, costa solo 29 euro ed è decisamente ideale per chi desideri sorvegliare uno spazio preciso. È infatti perfetto per controllare se è presente qualcuno all'interno dell'ambiente da spiare. E questo giocattolo vede perfino attraverso i muri.

Monitorare la presenza di una persona in un luogo è un



primo passo ma l'obiettivo di una spia è ascoltarla. Abbiamo trovato una coppia di walkie talkie di lunga portata in grado di trasmettere suoni a una distanza di 5 chilometri. Prezzo: 59 euro. Ora che l'audio c'è e la sorveglianza dell'ambiente anche, non mancano che le immagini. Come vedere senza essere visti? Non è difficile. I giapponesi di RF Systems hanno appena realizzato una telecamera miniaturizzata da 2,7 megapixel. L'occhio elettronico misura solo 3,5 cm. Le immagini vengono inviate senza l'impiego di cavi a una centralina provvista di uscita RCA. Lo strumento può essere utilizzato a distanza senza difficoltà. Abbiamo trovato un piccolo televisore con antenna integrata, al prezzo di 50 euro, che consente di ricevere le immagini inviate dalla micro-telecamera. E di micro-telecamere più o meno piccole su Internet se ne trovano a centinaia. Per esempio, abbiamo scoperto una "Wireless Camera" poco più grande di una palla da golf. È in grado di riprendere in piena notte e di intercettare ogni minimo suono. Prezzo: 80 euro.
Su Amazon abbiamo trovato una parabola per l'ascolto. Si tratta di un giocattolo da 69 euro che dovrebbe permettere ai bambini di ascoltare i suoni della natura, per esempio quelli degli uccellini. Al collaudo, il dispositivo si è rivelato in grado di rilevare perfettamente ogni rumore a una distanza di 100 metri. Interessante, specie se affiancato alla "macchina della verità" prodotta da Smarthome. Voice Stress Analyzer, questo il nome del dispositivo, permette di valutare se è probabile che la persona ascoltata stia mentendo. Il rilevatore in miniatura analizza infatti il livello di stress presente nella voce. Il prezzo è di 35 euro. Per la serie "sorveglianza selvaggia", ecco l'orologio-telecamera spia (Hidden Camera Spy Clock) disponibile su chinavision.com. All'interno del dispositivo è nascosta una telecamera a colori. Un ricevitore acquisisce le immagini e consente di registrarle in tempo reale. Il dispositivo è venduto a 50 euro. Meno discreto a causa della sua grossa antenna è il robot-spia Snooper. Distribuito a un prezzo di 40 euro, ascolta tutto ciò che avviene sotto la sua parabola, fino a una distanza di 50 metri. D'altronde, chi si preoccuperebbe di un giocattolo distribuito da iirobotics.com?



Passando agli occhiali da spia, ecco la "Sunglasses Camera with Personal Digital Video Recorder". Il dispositivo è venduto da spycatcheronline.co.uk e comprende una telecamera incorporata, un monitor a colori integrato, un altoparlante, 32 MB di memoria interna e un alloggio per una scheda di memoria SD/MMC che consente di salvare più immagini.
Per finire, il rilevatore di impronte digitali. Meglio che nei telefilm... Il Clue Spray prodotto da Brevis consente di rilevare le impronte di un estraneo su documenti, valigie eccetera. Lo spray consente di scoprire eventuali "mani indiscrete". "Applicate lo spray su un oggetto che ritenete possa essere stato manipolato dal sospettato. Volete sapere se l'oggetto è stato toccato? Utilizzate una lampada a luce ultravioletta per vedere le impronte digitali" - spiega l'inventore del prodotto.
Lo spray è in vendita a meno di 20 euro. In pratica, questi strumenti possono benissimo essere sfruttati da malintenzionati. Ai Mac Gyver dello spionaggio è ormai sufficiente ricorrere a questi giocattoli per avere la possibilità di raccogliere informazioni riservate. La prossima volta che vedremo il nostro fratellino, assicuriamoci che non abbia piazzato una macchinina o un orsetto nel nostro ufficio... ■



Il blogging secondo la BAIA DEI PIRATI

Un servizio rivolto ai blogger che vogliono esprimersi liberamente e senza censure? Si chiama Baywords e lo offre il noto tracker svedese The Pirate Bay

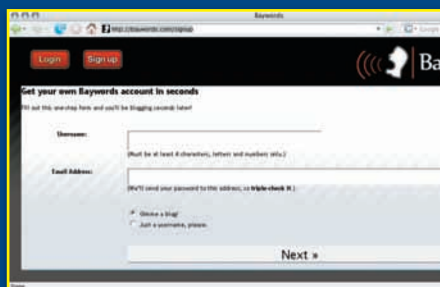
La polemica è l'anima del commercio e The Pirate Bay lo sa bene. È per questo che in aprile il noto "covo di pirati" ha lanciato una nuova iniziativa chiamata Baywords (http://baywords.com/).
Di cosa si tratta? Di un servizio gratuito per aprire un blog (o anche più di uno) in cui scrivere e pubblicare ciò che si vuole liberamente senza censure e senza filtri, ferme restanti le regolamentazioni della legge in Svezia, dove risiedono i server.
L'idea dei pirati è piaciuta tanto che a un mese dall'apertura erano già diecimila i blog aperti. Vediamo allora come crearne uno e cosa troveremo sul server di baywords.com

:: Registriamoci

Per attivare uno spazio proprio sulla home c'è il pulsante "Sign Up" in alto a sinistra. In alternativa si può andare all'indirizzo http://baywords.com/signup



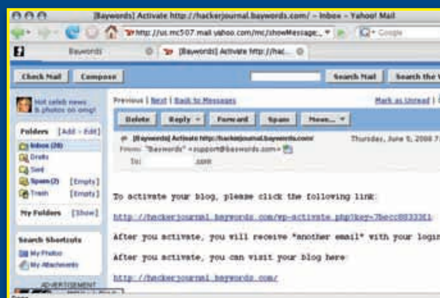
BLA BLA BLA,....
BLA BLA BLA,....
BLA BLA BLA,....



I campi richiesti sono solo due, il nome utente che si desidera e l'e-mail a cui verranno inviate le credenziali per l'accesso. La procedura serve anche solo per creare un'utenza senza blog, quindi accertarsi che sia selezionata l'opzione "Gimme a blog!". Alla pressione del gigantesco tasto "Next" in basso si arriva alla schermata in cui si deve scegliere il nome del blog e il nome del sottodominio (che sarà del tipo nomedelblog.baywords.com).



Anche qui c'è un'opzione, relativa all'indicizzazione sui motori di ricerca per blog e nello specifico Google e Technorati. La terza ed ultima schermata conferma la creazione del blog ma avverte che per scrivere è necessario attivarlo tramite il link in un messaggio spedito all'indirizzo e-mail fornito. L'attivazione va fatta entro 48 ore: in caso contrario tutta la procedura di registrazione scade e bisogna rifarla.

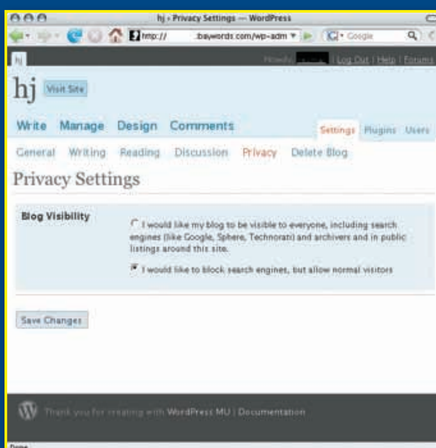


:: BayPress

Il clic sull'indirizzo nel messaggio porta ad una stringata schermata che conferma l'attivazione del blog e spiega che si può fare login con il nome utente scelto e una password, che verrà inviata sempre via e-mail.



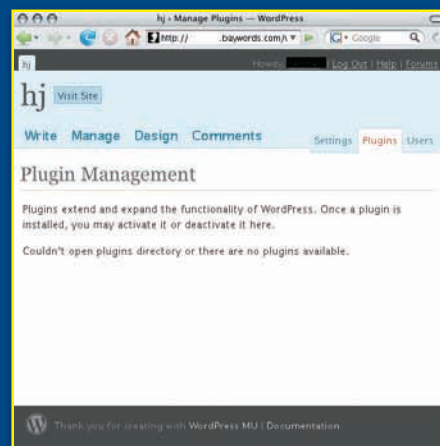
Già durante la procedura di registrazione vari elementi svelano quale sia la piattaforma adottata dagli svedesi ma dalla finestra di login diventa chiaro: quelli di Baywords sono dei blog basati sul noto WordPress nella variante MU (http://mu.wordpress.org/).



La versione di WordPress adottata è la recente 2.5 e ci sono tutti gli strumenti necessari a curare un blog: scrittura di post come di pagine, stilare un blogroll, gestione di quanto scritto, dei commenti e delle parole chiave (i tag) e delle categorie tematiche nonché di immagini ed altri file multimediali. Si può ovviamente cambiare l'aspetto per mezzo dei temi forniti, che sono ben 36. Non esagerato ma comunque sufficiente anche lo spazio fornito sul server, che è di 100MB.
Molto interessante è anche che al proprio nome utente si possono creare ed associare altri blog, con indirizzi diversi, sul server baywords.com.

:: I limiti

A guardare bene l'unico limite della piattaforma baywords è che non permette di installare nuovi temi o modificarli (inserendo codice personalizzato) e tantomeno ci sono plug-in.



I plug-in sono una delle "armi" di WordPress e ne estendono le funzionalità ma -probabilmente anche per motivi di sicurezza e semplicità di gestione- si è deciso di non fornirne e sul forum di supporto (http://suprbay.org/forumdisplay.php?f=56) brokep, storico fondatore della Baia dei pirati, ha confermato il no anche per il futuro.

IL CRIMINE PAGA?

Secondo un articolo di maggio su TorrentFreak http://torrentfreak.com/the-pirate-bay-100-popular-080518/
The Pirate Bay, con i suoi 25 milioni di visitatori mensili, si è ormai conquistato un posto tra i 100 domini Internet più visitati. Nella lista, che comprende nomi quali Google, Yahoo!, YouTube, FaceBook e Wikipedia oltre a The Pirate Bay c'è anche Mininova, attualmente in una posizione più alta, al cinquantaduesimo posto.

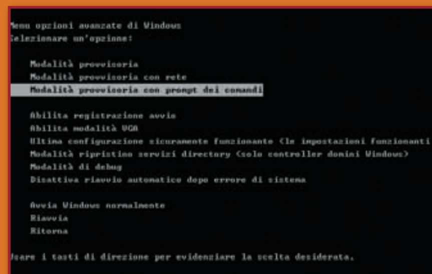
I NEMICI PUBBLICI

Metà anno, tempo di bilanci, vediamo chi ha fatto più danni nel primo semestre 2008

Eccoci a metà dell'anno pronti a stilare una classifica di quali sono stati i peggiori virus sulla rete nei primi sei mesi di questo 2008, resta sempre nella nostra top 5 Storm che con tutte le sue innumerevoli varianti continua a imperversare indisturbato.

:: Cutwail

Questa nuova generazione di trojan ha fatto la sua comparsa nell'aprile del 2007, ma da quel momento sono comparse numerose varianti che hanno reso il virus sempre più efficace e pericoloso. In particolare, le ultime versioni di Cutwail installano sul computer una versione aggiornata del modulo a cui il virus si affida per scaricare da Internet i suoi aggiornamenti o ulteriori virus. Attraverso questa tecnica, l'autore del trojan ha fatto in modo di garantire il funzionamento del virus anche se la macchina viene avviata in modalità provvisoria. Cutwail utilizza inoltre un rootkit in grado di "nascondere" ai programmi antivirus le modifiche che il virus apporta al registro di sistema. Oltre a scaricare file e programmi da Internet, il trojan si preoccupa di scandagliare l'intero disco fisso alla ricerca di qualsiasi documento possa contenere un indirizzo di posta elettronica. Una volta selezionati gli indirizzi email, Cutwail li memorizza in un file in formato TXT e trasmette il documento a un server.



Le nuove varianti di Cutwail sono in grado di funzionare anche se il computer viene avviato in modalità provvisoria, uno degli stratagemmi che consentono, di solito, di bloccare il funzionamento dei virus ed eliminarli dal sistema.

:: xo8wr9

Il nome del virus non è ancora disponibile e gli sviluppatori fanno riferimento a questa nuova minaccia con una sigla convenzionale. Si tratta, però, di uno dei rari virus che non si diffondono via Internet, ma preferiscono sfruttare un supporto "fisico", come avveniva alcuni anni fa con i floppy disk. In questo caso, però, xo8wr9 sfrutta le chiavi di memoria USB. Il virus modifica il file autorun in modo da avviarsi ogni volta che la chiave di memoria viene inserita in un computer che ha attiva la funzione di Avvio automatico. Oltre a immettere una copia di se stesso sulle unità disco collegate al PC, xo8wr9 stabilisce una connessione Internet nascosta. Quest'ultima è diretta a un server cinese, dal quale il virus scarica altri software dannosi, come spyware e trojan.

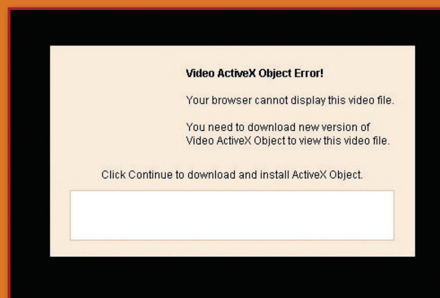


:: Zlob

Il virus è già conosciuto da mesi ma, a partire dalla metà di marzo, si sta diffondendo grazie a una nuova strategia che coinvolge migliaia di siti Web e sfrutta una "vecchia" vulnerabilità chiamata XSS o Cross Site Scripting. Si tratta, in pratica, di una tecnica che usa particolari script realizzati in Java in grado di funzionare tra una pagina Web e l'altra. Per attivare il codice è sufficiente che questo sia visualizzato su un sito vulnerabile agli



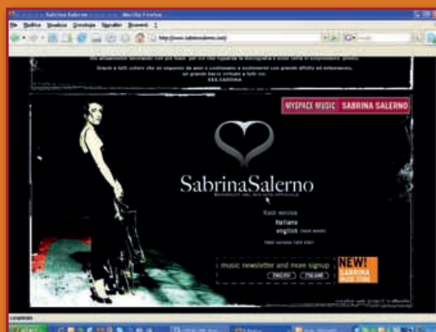
attacchi XSS. Lo stratagemma usato dai pirati informatici è molto elaborato ed estremamente efficace. Per prima cosa, viene individuato un sito molto frequentato che sia vulnerabile agli attacchi XSS e che mette a disposizione dei suoi visitatori un sistema di ricerca. I pirati analizzano il sito e creano il codice Java in grado di sfruttare la vulnerabilità. Il codice, poi, viene inserito direttamente nell'indirizzo di una pagina Web. Una volta completata questa fase, i pirati informatici hanno a disposizione tutto ciò che gli serve e devono solo fare in modo che l'indirizzo che contiene il codice venga visualizzato sul sito che hanno preso di mira. Qui entra in gioco il sistema di ricerca interno: la gran parte dei siti, infatti, sfrutta motori di ricerca esterni come Google. Ai pirati non rimane che inserire parole chiave molto popolari nella pagina Web e pubblicarla su Internet. Da questo momento sarà solo questione di tempo: quando un visitatore di quel particolare sito farà la ricerca "giusta", l'indirizzo della pagina Web verrà visualizzato e il codice si attiverà, dirottando il malcapitato su un'altra pagina Web. È qui che sul computer verranno installati una serie di virus e trojan, tra cui il temibile Zlob.



In alcuni casi, il virus Zlob viene installato tramite controlli ActiveX. Per eseguirli serve una conferma, ma il messaggio cerca di ingannarci facendoci credere che sia un innocuo video.

:: Italian Job 2

Ancora una volta la minaccia non è rappresentata da un virus specifico, ma da una sorta di "campagna" che ha travolto il nostro paese. Nel mese di maggio, infatti, gli esperti di sicurezza hanno identificato oltre 90 siti Web italiani infettati con un codice Java, chiamato JS.AFIR.A. Lo script agisce in maniera estremamente mirata: ogni volta che un computer si collega al sito, analizza la versione di Internet Explorer installata sulla macchina per verificare che si tratti di un computer con Windows in italiano. Solo se questa verifica è positiva, il codice si attiva e dirotta il computer su un altro sito Web. È da qui che si avvia l'installazione di due trojan, ai quali viene affiancato anche un rootkit. Molto probabilmente, l'aggressione avviata contro i computer italiani fa parte di una strategia che punta a creare una botnet, ovvero una rete di computer zombie, da utilizzare per campagne di spam o altri crimini informatici. Secondo una ricerca condotta da GData, l'Italia detiene già un poco invidiabile record in questo campo: il 10% delle macchine infette e utilizzate come bot sono infatti italiane. Per arginare il fenomeno è intervenuta anche Google. Gli indirizzi dei siti Web compromessi sono affiancati da un messaggio che avvisa della potenziale pericolosità del sito.



L'attacco portato ai siti Web italiani non ha risparmiato alcuni "nomi eccellenti", tra cui il sito ufficiale di Sabrina Salerno e un sito dedicato a Monica Bellucci.

:: Cioccolatini avvelenati

Le attese per il ritorno in grande stile del virus Storm non sono andate deluse. Con San Valentino è arrivata l'attesa nuova versione, che ha riservato anche qualche sorpresa. Il worm, infatti, gestisce la rete di computer infetti attraverso una tecnica simile al peer to peer, nella quale non c'è un server centrale che controlla tutti i computer "zombie".

Si tratta di una caratteristica che rende la rete di computer bot molto più resistente e autonoma. Secondo quanto raccontato da Mikko Hypponen, ricercatore di F-Secure, la botnet creata da Storm è programmata anche per reagire contro i computer che cercano di analizzare il funzionamento del virus. Quando individuano un computer infetto, infatti, gli sviluppatori di antivirus si collegano ripetutamente per scaricare il virus e analizzarne le varianti. Quando hanno provato a eseguire una simile procedura nei confronti di un PC colpito da Storm, la botnet ha "reagito": il computer usato dai ricercatori è stato infatti attaccato da centinaia di macchine, che lo hanno bersagliato usando un attacco Denial of Services.



BOTNET: diventeremo tutti zombie?

Nel folklore haitiano uno zombie è un morto resuscitato da uno stregone e ne svolge il lavoro sporco come un burattino. È proprio questa le fine che potrebbe fare il nostro computer in una rete botnet...

Tra le mille strategie pensate dagli hacker e dai pirati per dimostrare la loro abilità tecnica e accumulare capitali alle spese dei meno esperti, le reti botnet sono sicuramente tra le più ambiziose e potenti. Se, infatti, virus, trojan e worm possono essere considerati i singoli "criminali" del mondo informatico, le reti botnet sono più simili alla mafia o al terrorismo organizzato.

:: Virus contro bot

Una botnet è una rete di computer infettati da bot, termine inglese che deriva dall'abbreviazione della parola robot. Tra il malware tradizionale e i bot ci sono dei punti in comune. Entrambi si diffondono installandosi sui computer di ignari utenti connessi a Internet. Entrambi possono sfruttare vari canali per infiltrarsi nelle nostre macchine: scaricamenti da ftp o Internet, invio attraverso file torrent, allegati di e-mail, messaggistica istantanea come MSN o ICQ... Se, però, da una parte virus e compagni agiscono individualmente e in base a una programmazione definita e che rimane sempre uguale a se stessa, dall'altro i bot sono piccoli programmi indipendenti che però agiscono insieme sotto il controllo di una "mente" unica, la persona che controlla la rete botnet. Questa persona, ossia il botmaster o botherder (ossia "pastore di bot") avrà su un server remoto il software di controllo, detto in gergo Command and Control o C&C. I bot si infilano nei nostri computer e restano in attesa fino a quando il loro coordinatore non lancia, attraverso il C&C, un'azione combinata: si comportano in pratica come le cellule inattive di una rete terroristica.

:: Un mondo di possibilità

L'importanza delle botnet nel mondo della pirateria informatica è spesso sottovalutato. Prima di tutto, questi programmini riescono spesso a

infiltrarsi anche nei sistemi meglio protetti contro virus e altro malware. In secondo luogo, sono in grado di organizzare attacchi combinati su vasta scala. Per esempio, la maggior parte della cosiddetta junk mail, ossia i messaggi di posta indesiderata di cui tutti i computer del mondo vengono inondati, è gestita tramite botnet. A inviare le migliaia e migliaia (quando non milioni) di messaggi provvedono infatti i computer di ignari utenti, sotto il controllo di botmaster profumatamente retribuiti per i loro servizi. Questo tipo di sfruttamento di risorse non è l'unico rischio a cui è esposto il nostro computer. I bot possono infatti anche tenere sotto controllo la nostra tastiera per sottrarci le password di accesso ai siti, i dati della carta di credito o altre informazioni sensibili per rubare la nostra identità e i nostri fondi.

:: Tecno-estorsioni

Uno dei grandi cavalli di battaglia dei bot sono gli attacchi DDoS o Distributed Denial of Service (letteralmente "negazione di servizio distribuita"). Questo tipo di attacco usa una vera e propria inondazione di richieste per portare il funzionamento di un sistema informatico che fornisce un servizio, come per esempio un sito Internet, oltre il limite massimo delle sue prestazioni e di conseguenza bloccarlo. Se, per sferrare un attacco simile, il pirata usasse una propria rete di computer, sarebbe facile risalire a lui quindi è molto più pratico ed efficace diffondere dei bot con uno dei metodi che abbiamo citato in precedenza. Quando è stato raggiunto un numero abbastanza ampio di macchine (o in occasione di un particolare evento o a una certa data), il botmaster ordina a tutti i computer sotto il suo controllo (detti in gergo zombie) di inviare le richieste di servizio al bersaglio. Data la diffusione di computer con connessione a banda larga dotati di sistemi di protezione limitati, il fenomeno delle botnet usate per attacchi DDoS è sempre più ampio e ha proporzioni sempre più allarmanti. Lo scopo? Spesso l'estorsione. I pirati bloccano, per esempio, un sito commerciale e chiedono un "riscatto" per permettergli di tornare operativo. In altri casi gli attacchi DDoS sono usati come mezzo per paralizzare dei concorrenti o per manipolare degli eventi politici, bloccando per esempio il sito di un candidato il giorno delle elezioni.

:: Truffe e meta-truffe

Le botnet si possono usare anche per alterare i ritorni pubblicitari di un sito Internet. Per esempio, se il nostro sito commerciale contiene delle inserzioni "pay per click" (ossia in cui chi compra la pubblicità ci paga in base a quante persone cliccano sulla sua finestra o sul suo banner) o "pay per install" (in cui il cliente offre un programma e ci paga in base a quante persone lo installano), possiamo assoldare un botmaster per ottenere migliaia di clic e di installazioni da parte di utenti in realtà del tutto disinteressati al messaggio pubblicitario. Più facilmente, però, sarà un nostro sleale concorrente a valersi dei servizi di una botnet per farci avere un numero di clic o scaricamenti esagerati e rovinare la nostra reputazione con i clienti pubblicitari. Può sembrare paranoico ma è esattamente quello che è successo a Google qualche anno fa: accusato di negligenza per non aver installato le difese sufficienti a evitare che dei malintenzionati potessero manomettere la funzionalità delle sue inserzioni pubblicitarie, il motore di ricerca ha scelto di chiudere la causa pagando 90 milioni di dollari.

:: Il contagio si diffonde

Oltre a essere in grado di svolgere, come abbiamo visto, numerosi compiti, le botnet hanno la capacità di espandersi e aggiornarsi. Non solo i botmaster hanno la possibilità di inserire nell'intera rete i loro ultimi ritrovati ma possono usare i bot per cercare i computer più vulnerabili su cui espandersi. Man mano che cresce, inoltre, una rete botnet ha sempre più potenza e di conseguenza più capacità di espansione. Uno zombie tira l'altro...

:: Pirati in carriera

Uno degli aspetti più inquietanti del



LA COMUNNITY DEL MALWARE

Alcuni sviluppatori di botnet hanno persino adottato la strategia del codice open source. Questi pirati rendono pubblico il codice dei loro programmi, attorno ai quali si creano delle vere e proprie community pronte non solo a provare il prodotto e dare consigli su eventuali limiti o difetti, ma anche a collaborare attivamente al suo miglioramento aggiungendo parti di codice. Spesso i membri della community facilitano anche la diffusione internazionale dei bot traducendoli nelle loro lingue. Naturalmente i bot che possono appoggiarsi su una larga community sono ancora più difficili da individuare e bloccare perché godono di numerose varianti che rendono il lavoro di chi deve creare delle strategie di difesa una vera sfida.

fenomeno dei bot è che riescono a infiltrarsi anche in sistemi ben protetti. Spesso anche reti professionali ben difese contro vari tipi di virus e altri attacchi informatici cadono vittime degli attacchi dei bot e delle botnet. Il fatto è che questa forma di pirateria si sviluppa in un mercato molto ricco, con una clientela ampia e in grado di investire. Di conseguenza, è altamente specializzata e sofisticata non solo dal punto di vista tecnico ma anche da quello organizzativo. Prima di tutto, i programmatori che producono i bot hanno spesso conoscenze straordinarie e sfruttano tecniche d'avanguardia anche per gli standard industriali. L'ambiente, inoltre, è altamente competitivo e questi professionisti del malware "fanno a gara" a produrre i bot più efficaci o in grado di nascondersi meglio. Le tecniche usate per evitare che il server di gestione del C&C possa essere individuato e bloccato sono spesso molto elaborate. Per esempio ci possono essere diversi server centrali che assumono il controllo in ciclo, ciascuno per pochi minuti consecutivi, o un C&C primario può delegare la gestione della rete a più C&C secondari su server diversi. Una vera e propria gerarchia simile a quella usata in un'organizzazione militare.

:: Un mercato in crescita

Tanta professionalità sarebbe sprecata e difficilmente finanziabile se non ci fosse un mercato per le botnet. In realtà la loro flessibilità e potenza possono risultare utilissime a diversi "clienti". Oltre ovviamente ad hacker e spammer, possiamo contare la malavita organizzata, i gruppi terroristici, gli estremisti politici, i professionisti dello spionaggio industriale o chiunque abbia interesse, per esempio, a bloccare un servizio basato su Internet. Il mercato è talmente organizzato che ci sono dei mediatori professionisti a fare da interfaccia tra i tecnici e i loro clienti. Le transazioni avvengono in genere via chat o e-mail e, con i contatti giusti, possiamo letteralmente "affittare" una botnet per sferrare un attacco a nostra scelta attraverso decine se non centinaia di migliaia di computer. Negli Stati Uniti ci sono già stati diversi casi legali contro "distributori" di servizi basati su botnet e il livello di professionalità è semplicemente impressionante. Spesso sono in grado di fornire ai loro clienti prodotti ben testati e un servizio di assistenza tecnica.



:: Le contromisure

I fornitori di servizi Internet tipicamente bloccano gli attacchi DDoS con un metodo efficace quanto lesivo per il loro cliente. Quando si rendono conto che un dato URL è sotto attacco, ne dirottano il traffico su un indirizzo disattivo, facendo perdere di conseguenza al loro cliente anche i messaggi legittimi. Se contro gli attacchi DDoS possono quindi offrire una difesa, anche se con i suoi limiti, hanno risorse modeste per combattere le altre forme di danneggiamento e frode legati ai bot. Ci sono diverse aziende che si occupano della protezione contro i bot. Preparano dei computer vulnerabili che facciano da esca e, una volta che hanno attirato i bot, li studiano per trovare il modo per disattivarli. Sul mercato si trovano programmi antibot di aziende prestigiose ma avere una protezione completa per il nostro sistema non è impresa facile, dato che ne nascono sempre di nuovi e le organizzazioni che li gestiscono sono sempre più ricche e preparate. Dobbiamo quindi rassegnarci a un futuro da zombie? Certamente no. Conviene però dotarsi di un buon antibot, aggiornare costantemente i programmi in uso sul nostro computer per limitare al massimo il numero di falle e vulnerabilità e... tenere sempre gli occhi aperti.

FBI IN ALLERTA

Negli Stati Uniti le forze dell'ordine sono ben consapevoli del fenomeno delle botnet e dei rischi che esso comporta. Il 13 giugno dello scorso anno l'FBI ha pubblicato i risultati della prima parte dell'operazione BOT ROAST, un'indagine a livello nazionale tuttora in corso che al momento del comunicato aveva identificato oltre 1 milione di indirizzi IP di computer usati come zombie. L'FBI collabora con vari partner prestigiosi nella lotta contro le truffe informatiche e le botnet ma la situazione legale anche negli USA è tutt'altro che chiara. In pratica a venire investigati sono solo i casi che coinvolgono truffe di proporzioni imponenti o gravi danni ad aziende importanti e il resto della popolazione è lasciato a sé stesso e ai mezzi di difesa che è in grado di adottare privatamente. Anche quando il governo decide di intervenire, visto che le truffe vengono organizzate con migliaia di computer in diversi Paesi, i casi sono difficili da gestire perché assumono dimensioni internazionali e implicano quindi problemi di giurisdizione.



BARCODE ART

In Giappone quello per il codice a barre non è più uno spazio triste e serioso

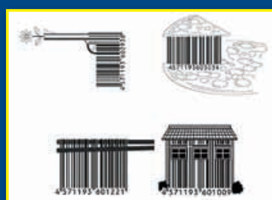
È semplice, rigoroso e minimale e lo troviamo ormai su gran parte delle confezioni in commercio: che sia uno snack o un server multiprocessore quelle le strisce e numeri in bianco e nero campeggiano immancabilmente con il loro carico neutro di informazioni. C'è addirittura chi, per la natura iconica del codice a barre, lo ha scelto per un tatuaggio, con inquietanti echi Orwelliani.



Ma il codice a barre non deve per forza essere uno spazio avulso dal resto della confezione né tantomeno compassato. Dal Giappone ci arrivano numerosi esempi che dimostrano come ci si può giocare e reinterpretarlo anche con ironia, ferma restando la leggibilità delle informazioni.



Il minimo comune denominatore infatti è che gli OCR riescano a scansionare e interpretare le righe (o almeno un pezzo) ma al di là di questo si è scoperto c'è libertà più assoluta. La libertà di trasformare il codice in un'onda cavalcata da un surfista, il profilo di un canyon o dei grattacieli di una città o in una pioggia da cui ci ripara un ombrello aperto. Oppure si può trasformare il tutto in una capanna o una pistola (da cui però sbuca un fiore) o ancora nel caso di prodotti alimentari integrare le linee del codice in un trancio di pizza (surgelata) o sposarlo con delle bacchette per mangiare degli spaghetti o tagliolini.



:: L'anima del commercio

Più in generale il codice a barre può e deve diventare una parte integrante e integrata nel design del prodotto che si vende, e nella pubblicità, come dimostrano i lavori dello studio nipponico d-barcode (http://www.d-barcode.com), raccolti anche in un volume (purtroppo esaurito).



Largo quindi oltre che alle illustrazioni anche al colore, per rendere meno serioso e anzi accattivante il codice a barre. In altre parole: creativi, non avete più scuse per lasciare così com'è quel rettangolo con righe e cifre!



Nicola D'Agostino
www.nicoladagostino.net

La velocità SI PAGA!!!

Che la situazione italiana dell'ADSL sia drammatica lo sappiamo, cerchiamo di capire meglio quanto e di trovare la migliore tariffa per noi

Quanto dovrebbe costare realmente un collegamento 24 ore su 24 in ADSL per tutti? In America, così come in molte zone si stanno diffondendo le coperture gratuite, finanziate magari con la pubblicità, mentre noi quasi ovunque dobbiamo ancora pagarci singolarmente l'abbonamento.
Tuttavia il costo di un servizio, al pari di qualunque altro prodotto, dovrebbe scendere proporzionalmente alla concorrenza che c'è nel mercato quando la maggior parte dei possibili acquirenti ha già comprato. E questo non succede in Italia e non succede soprattutto per l'ADSL. La causa principale è che l'ex-monopolista del settore, Telecom Italia S.p.A. continua ad essere il gestore unico (e unico proprietario) dell'infrastruttura denominata ultimo-miglio, il collegamento cioé tra le centrali (sempre di proprietà Telecom) e la presa telefonica all'interno dell'abitazione e dell'ufficio. Solitamente si tratta di un tratto in rame posato svariati anni fa, il cui costo di installazione è stato ampiamente ammortizzato e che non richiede particolare manutenzione. Certo, infiltrazioni d'acqua e roditori possono localmente creare dei problemi e quindi in quei casi si deve manutenere la tratta, ma in genere abitazioni anche degli anni Settanta continuano ad avere lo stesso rame inizialmente installato e sul quale viene offerto lo stesso il servizio ADSL. Il vantaggio di questa tecnologia risiede nella capacità di combinare sia la voce che il traffico dati sullo stesso cavo e di abbattere quindi molti costi. Ma tale vantaggio diventa anche il vincolo, perché appunto se durante il percorso un altro cablatore ha piazzato un bel chiodo proprio sul cavo, oppure l'umidità ha in parte rovinato il cavo senza però intaccare la capacità trasmissiva, avrò come conseguenza un decadimento di prestazioni che si misura in un modo davvero preciso: attraverso il rapporto segnale-rumo-



Ecco delle centrali da cui il nostro segnale ADSL si dirama



Altra centrale di smistamento, come si può vedere parliamo di edifici vecchi

re, ossia qual è l'attenuazione che riceve il segnale pur rimanendo intelligibile.
Questa unità di misura è particolarmente importante, perché è la stessa usata dai tecnici Telecom (o meglio, dai tecnici che lavorano per conto di Telecom e degli altri gestori dato che ormai è tutto gestito in outsourcing, cioé dato in appalto ad aziende esterne), per stabilire se intervenire su una certa linea dove c'è stata la segnalazione di collegamento lento (vedi tabella a pagina 22). In pratica, anche se si acquista un'ADSL con dichiarato massimo 7 Mbit/s di banda e si abita in un edificio non di recente costruzione, è probabile che non si arrivi neanche a 1 Mbit/s come ho sperimento personalmente pur avendo cambiato gestore ADSL. Ma anche qui, il cambio è fittizio perché la rete (tra i due cambi) resta sempre dello stesso proprietario (Telecom) e cambia solo l'azienda di interfaccia che ufficialmente mi sta rivendendo il servizio. Sono pochi i tratti in Italia alternativi a Telecom e solo nei grandi centri (come Fastweb in fibra ottica, non l'offerta Fastweb ADSL che è sempre su rete Telecom!). E di recente con l'UMTS e il WiMAX, che saltano completamente l'infrastruttura finale verso l'utente. A livello di centrali telefoniche sono stati affrontati molti costi negli ultimi 5 anni per aggiornare gli apparati e le aziende che rivendono l'ADSL di Telecom, sono in grado di offrire un'ottima assistenza tecnica perché con questi apparati intelligenti possono stabilire dal centro operativo la qualità del segnale fino alla centrale (e con modem acceso in casa possono verificare che in effetti un'utenza sta richiedendo il servizio). Il problema è dopo, per i problemi già visti e finché tale rete resterà di proprietà di un monopolista poco o nulla può cambiare da noi, che paghiamo le bollette ADSL più care d'Europa (oltre a un canone che a seguito delle liberalizzazioni è sempre meno giustificato). Quindi, in centrale la velocità continua a crescere, mentre il costo del servizio resta lo stesso elevato e la qualità non aumenta. Una situazione che può persino aggravarsi arrivando al paradosso: in grandi città, possono esserci dei buchi nella copertura del servizio causati dalla scelta operata in passato da Telecom per servire in fretta quartieri esplosi demograficamente. In quelle zone sono stati installati degli apparati multiplexer o apparati limitanti (concentratori), che permettono di offrire il collegamento voce a molte utenze e di contro non permettono assolutamente di aggiungere il servizio ADSL (es. Infernetto a Roma).



Quando vi dicono che ci sono problemi nella derivazione parlano di questo



Non tutte le citta possono vantare centrali come questa e restano senza ADSL

Quindi si fa un gran parlare di Anti Digital Divide, ma senza liberare completamente la rete non è possibile risolvere situazioni come questa dove il monopolista non ha alcun interesse ad investire per aumentare la copertura (perché caso per caso, un tecnico "Telecom" potrebbe sempre agganciarci a un'altra derivazione se disponibile in zona), mentre altri soggetti potrebbero offrire connettività a banda larga a un target ampio di potenziali clienti (si parla di una penetrazione reale di ADSL ferma al 17% in Italia, contro la previsione del 50% di appena 5 anni fa). E sempre Telecom tiene alto il costo di affitto della linea applicato anche agli altri provider nel caso di rivendita della linea e pari a 9€ al mese. È chiaro che con un tale canone di base non si può avere in Italia un'ADSL a 7,7€ al mese come hanno in Francia (con Talk Talk). Per la verità esistono già da tempo dei provider che offrono connettività a internet superando l'ultimo miglio via wifi (è possibile trovare una lista su www.antidigitaldivide.org) e/o offrendo connettività agli esclusi dall'ADSL, ma i costi sono ancora troppo elevati. In questi casi l'offerta più conveniente viene dai gestori mobili: si può sottoscrivere una flat (o semi-flat) su UMTS/HSDPA, ma si è soggetti a maggiori problemi di



congestione di rete, latenza e non c'è assolutamente alcuna banda minima garantita. Un grande aiuto che viene incontro a chi volesse trovare l'offerta migliore, viene dal sito di AltroConsumo che ha realizzato una pagina interattiva (http://www.altroconsumo.it/map/src/56931.htm) che permette di identificare l'offerta che fa al caso proprio in base alle proprie esigenze di connettività. Vengono così prese in considerazioni tutte le offerte ADSL così come quelle Dial-Up, ISDN e GPRS/UMTS. Nel momento in cui scrivo (escludendo promozioni valide solo sui mesi iniziali), per un collegamento costante 7 giorni su 7, viene identificata come più economica Tele2 con l'offerta flat a 16,90€ (che resta conveniente anche per connessioni di 4 ore al giorno) che è comunque il 120% più cara di Talk Talk. L'interesse continuo e crescente per la banda larga è motivato soprattutto dal peer-to-peer, a prescindere dalla legalità dei contenuti scaricati e gli operatori adottano politiche diverse per difendersi da una richiesta di banda che potenzialmente è a rischio con le infrastrutture attuali. Nella scelta dell'operatore va quindi verificato se l'ADSL fornita sarà in qualche modo limitata dall'operatore. Ma la sfida del momento è quella che si gioca con i contenuti che possono essere veicolati direttamente dal provider attraverso questi nuovi canali multimediali con il protocollo IPTV. Si stanno infatti diffondendo offerte di streaming video che fanno concorrenza sia alla televisione terrestre, che a quella satellitare. Storicamente, il primo gestore che ha offerto questo servizio in Italia è stato Fastweb. Quest'azienda ha investito e continua a investire su una propria rete in fibra ottica che lentamente è cresciuta e non è più presente solo a Roma e Milano, ma collega oramai diverse città. Per i suoi abbonati, oltre un vero collegamento a banda larga è possibile avere la TV ad alta definizione da anni e il telefono, sulla stessa linea e pagando un'unica fattura esattamente come gli abbonati alla TV via cavo degli USA, ma grazie al progressivo aumento di banda stanno aumentando le alternative. Il competitor diretto è sicuramente RossoAlice di Telecom (ora chiamato Yalp, http://www.yalp.it), che offre un palinsesto ben fornito di film e incontri sportivi.

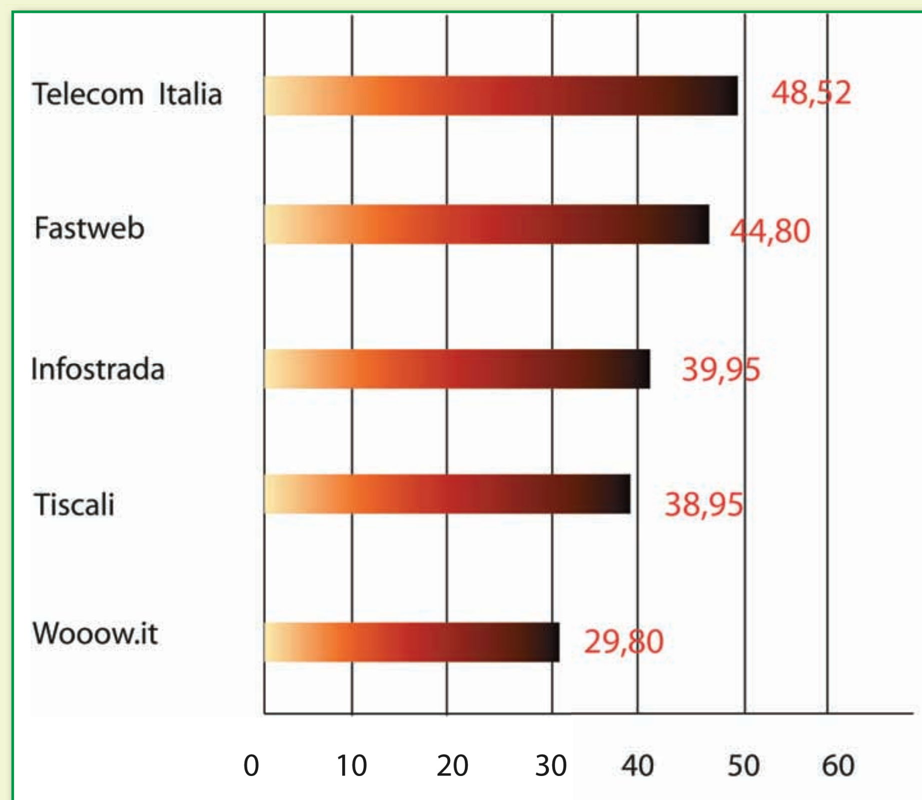
Tiscali (http://tv.tiscali.it) offre lo streaming dei canali digitali terrestri con pacchetti dedicati ai ragazzi e un servizio di replica di tutti i programmi trasmessi che possono essere rivisti per 48 ore dopo la prima messa in onda. Infostrada (http://tv.libero.it) oltre ai canali digitali terrestri instrada anche i pacchetti di Sky. Tele2 non è ancora partita in Italia con questo servizio (che offre ad



Ecco cosa si trova dentro gli armadi di Telecom... e poi ci lamnetiamo



In alcune zone le torri multiplexer non possono accettare canali ADSL perché dotate di vecchi sistemi



Ecco la tabella con la dimostrazione del decadimento del segnale a seconda dei vari operatori che abbiamo preso in esame







La nuova frontiera dell'offerta ADSL è nei servizi, come la TV





Altro discorso per webtv.coolstreaming.us, dai più considerato illegale

esempio in Francia), ma è stata di recente acquisita da Vodafone ed è possibile che vengano forniti nuovi servizi anche grazie alla convergenza con la rete mobile (e gli accordi già stretti tra Vodafone e RAI/Mediaset/SKY). Infatti è stata già presentata la Vodafone Station, un router ADSL 2+ che integra una porta USB sulla quale agganciare un modem HSDPA utilizzabile anche su un qualunque PC che dovrebbe offrire il collegamento a banda larga finché non si viene raggiunti da un collegamento via cavo per l'ADSL. A margine vorrei indicare anche uno tra i siti non ufficiali che permettono di godere di visioni in streaming come http://webtv.coolstreaming.us. Questo è diventato particolarmente famoso per gli amanti di eventi calcistici perché in passato (e forse in futuro replicherà) ha trasmesso partite mandate in onda anche all'estero e riversate quasi in tempo reale via internet. Siti come questo vengono posti sotto sequestro dalla Polizia Postale, dal momento che esistono degli accordi sui diritti televisivi (pagati fior fiore di euro dalle televisioni) che richiedono un abbonamento a pagamento per esser visti in Italia, ma se il sito si trova all'estero (o comunque sotto giurisdizione estera) è difficile o impossibile che venga oscurato. In questi casi viene intimato il blocco degli indirizzi di questi siti ai provider italiani in modo che non siano comunque raggiungibili, o almeno che sia più difficile raggiungerli. A San Frascisco, Google ha pagato di tasca sua la copertura wi-fi di tutta la città e offre un collegamento gratuito. Questo significa che tutti gli abitanti possono accedere liberamente alla rete senza dover sostenere alcun costo. Nel nord Europa, da tempo, esistono interi quartieri che hanno una copertura simile gestita per palazzine e dove il costo mensile per famiglia è irrisorio e ci sono progetti interessantissimi come http://www.free-hotspot.com e http://www.fon.com. In Italia spero che grazie al WiMAX (vedi articolo su HJ 151) sia possibile scuotere un mercato un po' troppo statico e forse ancora poco liberalizzato. Vorrei anche io una copertura a banda larga (a prescindere che sia o no completamente in ADSL) per tutti i cittadini anche perché se la pubblica amministrazione continua a procedere progressivamente nell'informatizzazione dei servizi erogati, potremmo ricevere tutti dei benefici derivati dall'accesso tramite internet a tali servizi (ove possibile erogarli), soprattutto in termini di tempo, ma anche di costi sostenuti dalla collettività. Si pensi ad esempio alla prenotazione di esami presso le ASL o l'emissione di certificati catastali, anagrafici, per non parlare delle comunicazioni tra diversi enti pubblici. Le tecnologie esistono e qualche passo è stato già fatto per cui voglio essere ottimista.

Massimiliano Brasile



La Fonera si può quasi considerare un competitors di Telecom e soci visto il servizio che offre



BUTTA I DATI nella rete

Sono sempre di più i sistemi di backup presenti in rete, ma sono realmente più sicuri del nostro hard disk??? Scopriamolo

Per proteggere i dati, non solo dobbiamo farne varie copie, ma anche archiviarli in posti diversi. Nessuno è al sicuro da furti o incendi. Dare DVD o dischi fissi di backup ad amici o metterli nella nostra seconda casa può essere una soluzione, ma dal punto di vista pratico è poco comoda e ci impedisce l'aggiornamento frequente dei contenuti. Comunque, niente garantisce che i DVD che abbiamo masterizzato saranno ancora leggibili fra qualche anno, visto la scarsa affidabilità di questi supporti. Per risolvere il problema, la soluzione migliore è usare il nostro collegamento Web a banda larga per trasferire periodicamente i file in uno spazio di archiviazione "remoto".

:: Backup sicuri al 100%

Per i dati confidenziali, il backup online non è consigliabile, se non possiamo contare sulla sicurezza offerta dall'azienda a cui ci affidiamo.
E la sicurezza ha un costo. Ecco perché le soluzioni che presentiamo, anche se a un prezzo relativamente abbordabile (circa 4 euro al mese) sono a pagamento. Il costo si basa sullo spazio disponibile, più o meno limitato, ma con la protezione garantita. Per esempio, con il sito Neobe Backup i dati vengono codificati prima che escano dal nostro computer e immagazzinati nel data center. È questa azienda a garantirne la protezione con un sistema anti-intrusione, una protezione contro gli incendi e la videosorveglianza... Peccato che non tutti siano così trasparenti. Per esempio, con Carbonite o con MozyHome Unlimited è difficile sapere che misure vengono usate per proteggere i nostri dati. È da notare che, nonostante siano tutti contratti a pagamento, pochissimi garantiscono al 100% la restituzione dei dati. Se vengono persi, è impossibile ottenere risarcimenti. Per avere una copertura assicurativa, con Neobe dobbiamo pagare 12 euro in più al mese per pacchetti da 5 GB (Platinum plan), quindi i costi cambiano! Il backup online funziona, ma si fa ancora fatica a trovare il giusto equilibrio economico. Le offerte interessanti non sono del tutto infallibili e quelle completamente sicure

costano tanto. Basta prendere per esempio l'azienda Foreversafe che, dopo tre anni di attività, ha dovuto chiudere bottega per debiti... Inoltre l'offerta soffre ancora della relativa lentezza dei collegamenti. Anche con l'ADSL, la capacità di trasmissione media è di appena 512 Kbit/s (1 Mbit/s al massimo).

Una lentezza che aumenta moltissimo i tempi di trasferimento. Comunque il programma Carbonite ci avverte: non più di 2 o 3 GB di dati al giorno. Abbiamo avuto conferma di questo dato durante i nostri test. Infatti, in sei ore, siamo riusciti a trasferire solo 1 GB di foto.

:: Soluzioni gratuite

Se non siamo troppo ansiosi, possiamo sfruttare i servizi gratuiti. Altrimenti possiamo usare la nostra posta elettronica come archivio dati. Infatti, da quando nel 2004, con il servizio GMail, Google ha lanciato la corsa all'archiviazione (che allora offriva 1 GB, contro i pochi MB della concorrenza), le caselle di posta elettronica sono diventate sempre più capienti. Livemail di Microsoft (la vecchia Hotmail) offre 5 GB e Google ha rilanciato con 6 GB. Yahoo!, che offre un'archiviazione illimitata, verrà presto raggiunto... Un'ottima occasione per archiviare i nostri dati e averli a disposizione con qualsiasi programma di navigazione e con qualsiasi PC collegato al Web. Comunque, facciamo attenzione.

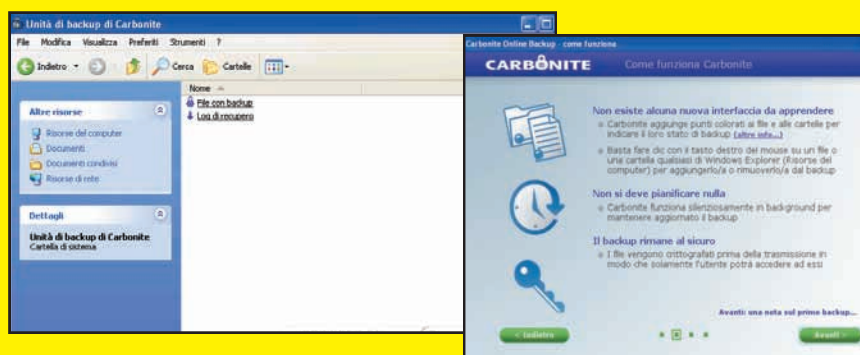
Le spedizioni non possono superare i 20 MB. Quindi dovremo limitarci alle foto, ai documenti e ai file audio. Niente film interi, sono troppo grandi! Se abbiamo un account GMail, possiamo anche installare l'applicazione gratuita GMail Drive (vedi riquadro "I consigli per il salvataggio online") per facilitare i trasferimenti. Infine, se vogliamo archiviare foto, esistono siti molto pratici dedicati a questo scopo. Per esempio, Google Picasa Albums Web archivia gratuitamente fino a 1 GB di foto online. Una soluzione alternativa da prendere seriamente in considerazione!

Salviamo i nostri dati con Carbonite 3

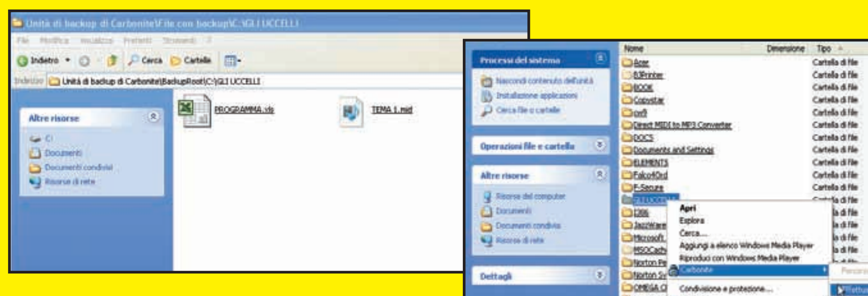
Facilissimo da usare, questo programma è efficace. Selezioniamo le nostre cartelle o i file importanti e Carbonite li mette al sicuro automaticamente su server protetti. Anche il ripristino è semplicissimo.



1 Scarichiamo il programma su www.carbonite.it (versione di prova gratuita per 30 giorno o a 49,90 euro all'anno). Finita l'installazione, appare l'interfaccia. È meglio scegliere la selezione manuale degli elementi da salvare.



2 Per aggiungere altre cartelle, clicchiamo con il pulsante destro sull'elemento desiderato e poi, nel menu contestuale scegliamo l'opzione di salvataggio di Carbonite. Accanto agli elementi selezionati appaiono dei cerchietti colorati che indicano il livello di salvataggio (finito, in corso...).



3 Andiamo nell'InfoCenter e poi, nella pagina di ripristino, scegliamo i file da ripristinare. Possiamo anche usare l'icona del lettore Carbonite che si trova sul desktop. Mettiamo il programma in modalità recupero per fermare il salvataggio mentre ripristiniamo i nostri file.

Immagini che parlano

La crittografia è oggi molto diffusa, ma la steganografia è da sempre una tecnica altrettanto valida per nascondere le informazioni

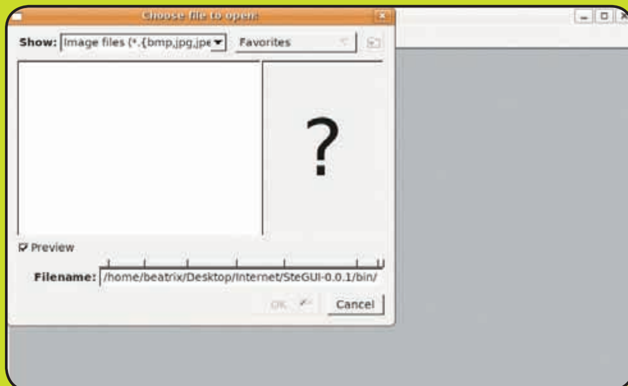


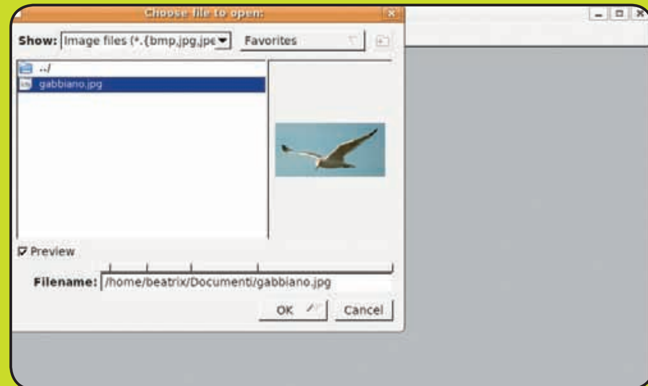
Il vantaggio essenziale della tecnica stenografica applicata alla telematica è che si evita l'instaurarsi di un canale di comunicazione tra mittente e destinatario; di un'immagine presente in Internet non è possibile ricostruire la provenienza, diversamente da un'immagine spedita via e-mail. La steganografia informatica necessita di due file. Il primo è un qualsiasi file, chiamato cover file (file di copertura). Il secondo è quello che si vuole tenere segreto, incorporandolo nel primo con il payload (carico, messaggio nascosto). Non ci sono restrizioni al formato del file segreto. Un requisito importante affinché la steganografia lavori in maniera ottimale è che i formati dei cover file siano di grandi dimensioni. Per nascondere un testo segreto di 200 KB, la dimensione del file di copertura deve essere almeno di 1 MB. Infatti, la maggior parte delle applicazioni steganografiche mostra un avvertimento se la dimensione del file di copertura risulta troppo piccola per nascondere effettivamente il payload. In sostanza nel file di copertura è necessario che sia presente una quantità sufficiente di dati ridondanti. È proprio alterando queste informazioni e combinando il risultato con il file nascosto che si pone in essere l'occultamento del file. In sostanza la quantità di informazione ridondante influisce sulla qualità del file di copertura, ma anche sulla sua capacità di nascondere informazioni. È per questo motivo che si scelgono file di copertura di grandi dimensioni e che raramente viene utilizzato un file di testo. Inoltre questi tipi di file sono soggetti alla perdita di informazioni nel caso di cambiamenti della formattazione del testo o di compressione.

::Tecniche di steganografia

Un file steganografato con successo non deve mai insospettire una persona che lo guarda o l'ascolta (sì, si possono nascondere informazioni anche nei file audio). La steganografia basata su immagini sfrutta l'incapacità dell'occhio umano di cogliere le piccole sfumature. Così con immagini a 24 bit, che utilizzano 16 milioni di colori è possibile alterare la composizione del file senza che si possa cogliere la differenza a occhio nudo. Con la tecnica del Least Significant Bit (LSB) (ultimo bit significativo) si va a sostituire l'ultimo bit di ogni byte. L'immagine risulta alterata in modo non percepibile. Il problema è che in questo modo i file hanno grandi dimensioni, ostacolandone la trasmissione. Usando degli algoritmi di compressione bisogna scegliere quelli senza perdita di informazione come GIF o TIFF, poiché con la compressione di tipo JPEG, che opera proprio sugli ultimi bit significativi, si rischia di perdere anche parte del messaggio nascosto. Anche i file di audio digitale possono essere usati come file di copertura. Il formato audio più ampiamente usato è l'AIFF e la sua variante WAVE. In questi lo spazio "usabile" nel file è generalmente tanto più grande quanto più è alta la frequenza di campionamento. Anche il formato MP3 è largamente usato, esso si basa sulla codifica delle sole parti di suono che possono essere percepite dall'orecchio umano, i suoni più alti

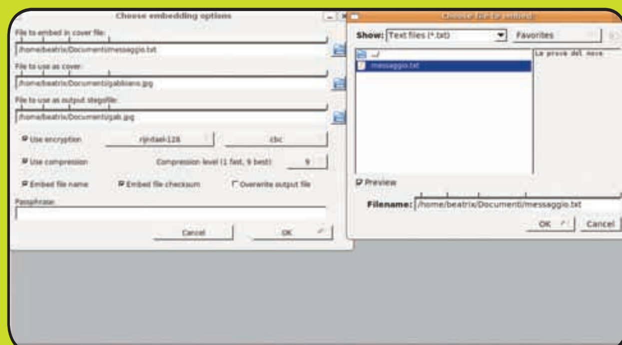
UTILIZZO DI STEGUI

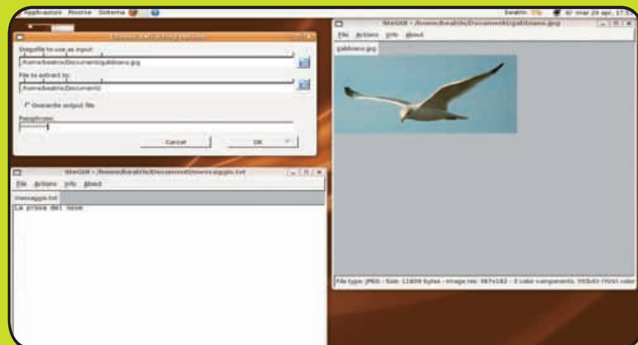




1 Nella cartella /bin è presente l'eseguibile di SteGUI, lanciandolo si apre una interfaccia grafica, in cui è possibile scegliere un file di copertura. Questo può essere scelto sia tra le immagini che tra i file audio.

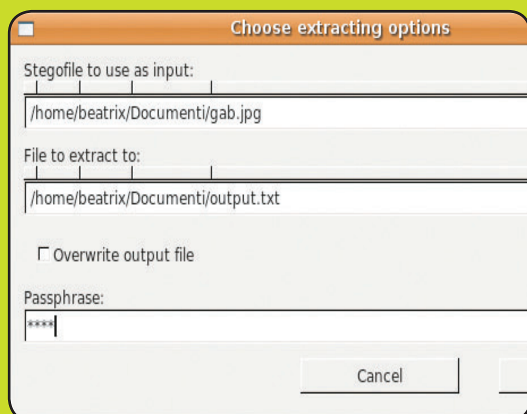
2 L'operazione successiva alla scelta del file di copertura è inglobare al suo interno il file da nascondere. Utilizzando l'editor di testo si realizza un file con estensione .txt dal menu Actions D Embed.





3 In questa finestra si inserisce il messaggio da inglobare, il percorso per l'immagine di copertura e il nome del file risultante (gab.jpg). Si possono scegliere diversi livelli di crittografia e di compressione, nonché inserire il nome del file e il suo checksum.

4 Il passo successivo prevede l'inserimento di una passphrase, una chiave necessaria per eseguire in modo sicuro il processo steganografico e che sarà utilizzata nel processo inverso per recuperare le informazioni nascoste.

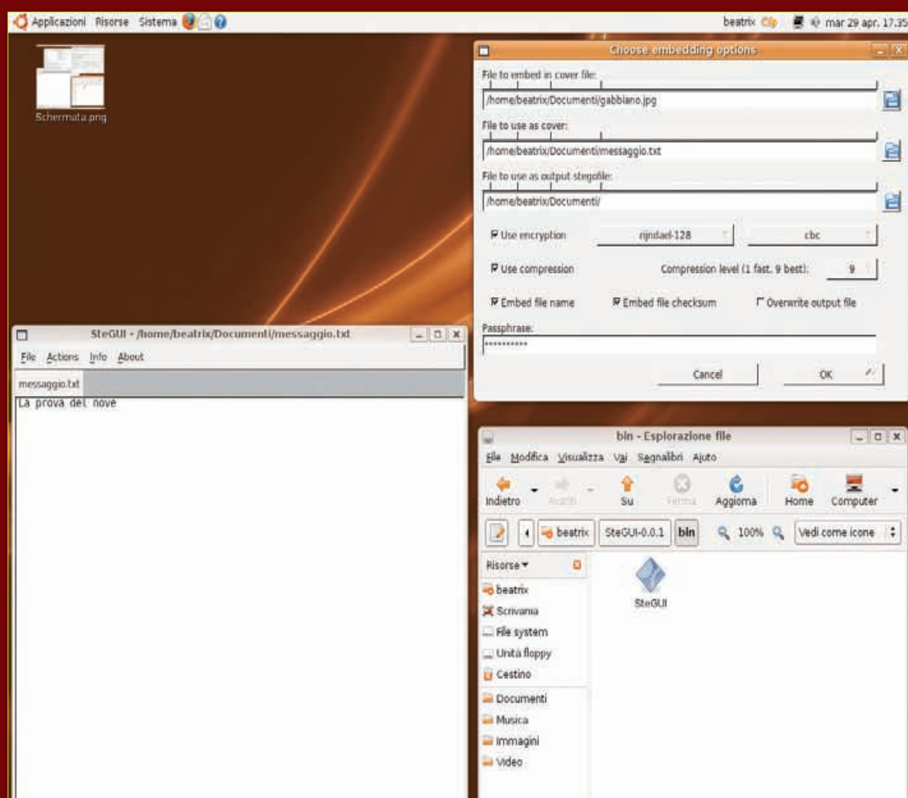


5 Per quanto riguarda la procedura contraria, ottenere il file in chiaro da quello steganografato, c'è bisogno degli stessi software e della passphrase definita dal mittente al momento dell'invio del file. Si usa Actions D Extract. SteGUI è un tool molto utile soprattutto per chi è abituato alle interfacce grafiche, i risultati sono ottimi e come si può osservare ad occhio nudo non c'è nessuna differenza tra i due file (gabbiano.jpg e gab.jpg) eppure uno di essi ingloba un messaggio nascosto. È sempre possibile modificare i file di testo con l'editor di testo incorporato, che supporta le operazioni di selezione, copia e incolla e permette all'utente di salvare i file modificati. Qualsiasi file venga aperto che non è riconosciuto come uno dei tipi supportati viene passato all'editor di testo e aperto come testo, come succederebbe con qualsiasi altro editor. Il riconoscimento dei tipi di file avviene leggendo l'header del file per i formati supportati, non controllando l'estensione del file, né usando altri procedimenti euristici dipendenti dal sistema.

no percepiti meglio di quelli più bassi e perciò è più facile nascondere i dati tra i suoni bassi senza che l'orecchio umano noti alterazioni. Nel caso dei file audio le tecniche steganografiche usate sono la Least Significant Bit (LSB) oppure la Low-bit Encoding (codifica del bit basso) per incorporare i dati da occultare nei bit meno significativi. La capacità di trasmissione del canale in questo caso è di solito pari a 1 Kbps per kilohertz, ma è semplice perdere informazione a causa dell'interferenza e della riquantizzazione. Una tecnica più sicura è chiamata Spread Spectrum e attraverso il suo uso il messaggio è codificato attraverso l'intera frequenza di spettro. Il file audio è quindi trasmesso su varie frequenze, che cambiano secondo il metodo usato, uno di questi è il Direct Sequence Spread Spectrum; questo metodo moltiplica il segnale attraverso una sequenza pseudo-casuale chiamata chip prima che sia trasmesso; il rischio è quello di introdurre interferenze nel suono, con la conseguente perdita di dati.

:. Sicurezza

Come molti strumenti di sicurezza, la steganografia può essere usata per differenti ragioni, alcune legali altre meno. Tra gli usi legittimi rientrano le filigrane digitali (Digital Watermarking), simili alla steganografia in quanto esse sono sovrapposte ai file; l'obiettivo è quello di assicurare la riservatezza delle informazioni importanti, di proteggere i dati da possibili sabotaggi, furti o sguardi non autorizzati. Ma è possibile anche un utilizzo illecito, permettendo, ad esempio, comportamenti non autorizzati. Generalmente non è possibile evitare queste azioni. Se qualcuno ha deciso di nascondere i propri dati, probabilmente riuscirà nel proprio intento. Quello che un amministratore di sistema potrebbe fare è giocare d'anticipo settando delle regole specifiche e restrittive sull'installazione di programmi non autorizzati. Si è detto che i file di grandi dimensioni sono i file preferiti dagli steganografi, di conseguenza all'aumento non giustificato del traffico passante attraverso un canale di comunicazione, l'amministratore di sistema deve quanto meno insospettirsi e usare gli strumenti per il rilevamento delle intrusioni per rilevare i movimenti e i comportamenti dell'utenza.



Ecco la semplice interfaccia utente di SteGUI

:: Steghide

Un tool veramente interessante per realizzare la steganografia in ambiente GNU/Linux e Windows è Steghide (http://steghide.sourceforge.net/documentation.php), scritto in C++ da Stefan Hetzl. È rilasciato sotto licenza GNU/GPL. Permette agli utenti di sfruttare le immagini Bitmap e JPEG (con la libreria Libjpeg) di Windows, i Wave di Windows e i file audio AU di Sun/NeXT come file di copertura; come payload può essere usato ogni tipo di file. I dati possono essere cifrati (usando le librerie MCrypt e MHash) e compressi (grazie alla libreria Zlib). In aggiunta ai dati veri e propri è anche possibile includere nel file steganografato il nome del file occultato e un checksum per verificare l'integrità dei dati estratti. Ecco un esempio pratico di Steghide. Due sono i file utilizzati: un'immagine (gabbiano.jpg) e un testo che si vuole nascondere nell'immagine (ad esempio: lista_password.txt). In Ubuntu è sufficiente lanciare il comando apt-get install steghide per installare il programma. Dopo l'installazione lanciate il seguente comando:

```
$ steghide embed -cf gabbiano.jpg
 -ef lista_password.txt
  Enter passphrase:
  Re-Enter passphrase:
  embedding "lista_password.txt"
in "gab.jpg"... done
```

Questo comando inserirà il file lista_password.txt nel file di copertura gabbiano.jpg. Gli argomenti -cf specifica il file di copertura, mentre -ef il file nascosto. Il comando embed è usato per inserire un payload in un file di copertura. In aggiunta alla crittografia e al checksum menzionati, si può anche proteggere i dati con una passphrase, che sarà richiesta al destinatario per l'estrazione dei dati nascosti. In questa fase

è possibile anche scegliere il livello di compressione da usare per il payload tra i nove forniti dalla libreria Zlib, così come l'algoritmo di crittografia e la modalità operativa. Attraverso un generatore di numeri pseudo-causali, inizializzata con la passphrase, viene creata una sequenza di pixel nel file di copertura. In questa saranno incorporati i dati da nascondere. Le celle che contengono i pixel corretti vengono ordinate. Attraverso un algoritmo di confronto basato sulla teoria dei grafi vengono trovate coppie di posizioni che permettono lo scambio di valori, in cui è possibile incorporare anche i dati segreti. Questo scambio fa in modo che la percentuale di colore presente nell'immagine resti invariata. Stessa procedura viene utilizzata per i file audio, considerando anziché i pixel i campioni audio. L'algoritmo di crittografia predefinito è il Rijndael con chiave a 128 bit, che si basa sullo standard crittografico AES (Advanced Encryption Standard) nella modalità cipher block chaining, cioè i blocchi di testo cifrato sono "incatenati" ai propri predecessori. In ogni caso è possibile selezionare qualsiasi algoritmo tra 18 possibilità (arcfour, wake, enigma, stream, cast-128, gost, rijndael-128, twofish, cast-256, loki97, rijndael-192, saferplus, des, rijndael-256, serpent, xtea, blowfish, rc2), ognuna delle quali può operare in vari modi. Per avere un elenco completo degli algoritmi e delle modalità operative si può eseguire steghide --encinfo. Dopo aver racchiuso il dato da nascondere si può inviare l'immagine al destinatario, che una volta ricevuta potrà estrarre il messaggio segreto. Infatti il destinatario userà Steghide in questo modo:

```
$ steghide extract -sf gabbia-
no.jpg
  Enter passphrase:
  wrote extracted data to
"lista_password.txt".
```

Se la passphrase inviata è corretta, il contenuto del file originale lista_password.txt sarà estratto dall'immagine steganografata e sarà salvato nella directory corrente. Se si è ricevuto un file che contiene file nascosti e si vuole ottenere informazioni aggiuntive prima di procedere con l'operazione di estrazione, si può lanciare il seguente comando:

```
root@desktop:/home/beatrix/
Documenti#
 steghide info gab.jpg
 "gab.jpg":
   format: jpeg
   capacity: 332,0 Byte
  Try to get information about
embedded data ? (y/n) y
  Enter passphrase:
   embedded file "messaggio.txt":
    size: 18,0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

Dopo aver esaminato queste informazioni generali come il formato e la capacità, Steghide può ottenere informazioni circa i dati racchiusi, rispondendo di sì e inserendo la passphrase, si visualizzeranno ulteriori informazioni.

:: SteGUI

Per chi fosse abituato alle interfacce grafiche, ecco SteGUI (http://stegui.sourceforge.net/), un tool grafico basato su Steghide. SteGUI è stato sviluppato da Nicola Cocchiaro, sotto licenza GNU General Public License. Per installare SteGUI è necessario fare alcuni passi essenziali. Infatti sono necessarie le seguenti librerie, da scaricare e installare con il solito sistema di pacchettizzazione. In Ubuntu, ad esempio si usa apt-get install [nome pacchetto] dove [nome pacchetto] deve essere:

- per le librerie FLTK (www.fltk.org) - libfltk1.1-dev
- per Pstreams (http://pstreams.sf.net/) - libpstreams-dev
- per ALSA Project (www.alsa-project.org) - alsa-base e alsa-utils
- per Libjpeg (www.ijg.org) - libjpeg62-dev

Per costruire la GUI è stato usato il toolkit FLTK. Scritto in C++, permette uno sviluppo rapido e indipendente dalla piattaforma (FLTK è disponibile per Linux, Windows e Mac OS X). È anche possibile fare uso di grafica 3D con l'emulazione OpenGL e GLUT. Le interface grafiche con Steghide attraverso la libreria PStreams, anch'esse scritte in C++, permettono di lanciare i programmi da ogni applicazione e trasferire i dati tra il chiamante e il chiamato, in modo simile alle pipeline della shell. Per la riproduzione audio è stata scelta la libreria ALSA, poiché è lo standard attuale sui sistemi Linux basati sul kernel 2.6. ALSA lascia allo spazio utente tutto quello che non appartiene al livello hardware, permettendo l'accesso alle caratteristiche del sistema audio con un'API che è indipendente dal driver effettivamente impiegato; sfortunatamente non è supportata dai sistemi Windows. Recuperate dal sito di SteGUI il file SteGUI-0.5.1.tgz, decomprimetelo, entrate nella cartella che si viene a creare e lanciate il comando:

```
root@desktop:/home/beatrix/
Desktop/Internet/
 SteGUI-0.5.1# make all g++
`fltk-config
 --use-images --ldflags` -lasound -
lm -lpthread
 src/Callback.o src/CardWidget.o
src/EmbedWindow.o
 src/ExtractWindow.o src/ImgWidget.
o src/MsgWindow.o
 src/PlayerPanel.o src/SndWidget.o
src/SteGUI.o
 src/StegWindow.o src/Support.o
src/TxtWidget.o
 src/Player.o -o bin/SteGUI
```

Se sono stati effettuati correttamente tutti i passi su descritti, nella stessa cartella SteGUI sarà presente una cartella bin, con il binario pronto all'uso.

```
$ bin/steGUI
```

:: Conclusioni

Come tutti gli strumenti, la steganografia, può essere usata a fin di bene oppure per fini illegali. Nel primo caso può risultare molto utile per la protezione dei dati e del diritto d'autore, ma nell'altro caso può rendere molto difficile l'individuazione di piani e progetti criminali. lxp

CONOSCI IL

SPYWARE

Questo tipo di minaccia informatica è tra le più difficili da estirpare. Sembra che i creatori di spyware spendano più tempo nel cercare di rendere immortali questi programmi che a sviluppare tecniche per nasconderli

Uno spyware è un tipo di programma che permette di raccogliere informazioni su una persona o su un'organizzazione anche a loro insaputa. Su Internet, uno spyware è un programma che raccoglie e trasmette informazioni sul comportamento dell'utente anche senza che questi lo sappia. Alcuni programmi legittimi comprendono addirittura una clausola di "consenso all'installazione" di veri e propri spyware nei loro termini di utilizzo.

È importante sapere che cosa si sta installando e leggere tutti i documenti di installazione prima di procedere, perché non sempre la disinstallazione è sufficiente a rimuovere gli spyware. Nella maggior parte dei casi, Adware, Spyware e Foistware hanno comportamenti e funzioni interconnesse e vengono comunemente definiti con il termine collettivo di spyware. Vediamo come funzionano...

:: Adware

Un adware può essere invasivo, nel senso che può disturbare l'utente, oppure può mostrare solo banner in un programma. Spesso viene installato a insaputa dell'utente e produce generalmente finestre pubblicitarie. Può anche raccogliere informazioni sull'utente e inviarle ad aziende che vendono pubblicità: in questo caso è uno spyware in tutto e per tutto.

:: Spyware

Lo spyware vero e proprio è un parente non molto lontano dell'adware, nel senso che anch'esso viene installato inconsapevolmente dall'utente. Spesso viene presentato come "accessorio gratuito", "acceleratore Web" e in alcuni casi perfino come "strumento per l'eliminazione di spyware". Sfortunatamente, questo tipo di spyware ha un obiettivo maligno, quello di raccogliere e registrare le informazioni che l'utente fornisce ad altri siti e a volte, come un virus, può essere in grado di registrare le sequenze di tasti premute.

:: Foistware

È un termine che indica i un tipo particolare di programmi spia. In particolare, si chiamano Foistware quegli spyware che fanno parte integrante di altri programmi (legittimi) che smettono di funzionare se lo spyware che installano viene eliminato. In pratica, per usare quel programma, dobbiamo per forza lasciare attivo lo spyware abbinato. Un tipico esempio di strumenti che usano foistware è Kazaa, il programma di condivisione file, ma anche GetRight (l'applicazione per riprendere gli scaricamenti interrotti) è stato per anni un baluardo della distribuzione di programmi che raccoglievano dati sugli utenti. In entrambi i casi la raccolta dei dati era richiesta per contratto al momento dell'installazione.

:: Problematiche non da poco

Uno spyware può teoricamente fornire a utenti malintenzionati le nostre informazioni personali più riservate. Per esempio, una normale visita a una banca on-line potrebbe fornire a un utente malintenzionato le nostre informazioni bancarie. Allo stesso modo, visitando il sito della nostra carta di credito forniremo alla spia le informazioni relative alla nostra carta. Questo è reso possibile dal fatto che alcuni spyware reindirizzano le informazioni che l'utente fornisce tramite un modulo Web a un altro sito, registrano i dati e inviano una copia delle informazioni al sito giusto. Senza creare questi problemi seri, lo spyware può comunque danneggiarci mandando a terzi informazioni su quello che vediamo sul Web e per contro mostrarci tramite il programma di navigazione contenuti pubblicitari fastidiosi. È noto inoltre che gli spyware rallentano i computer e bloccano alcuni programmi. Alcuni spyware alterano la pagina iniziale e "dirottano" i motori di ricerca. In altri casi, installano nel programma di navigazione una barra degli strumenti superflua. Il sintomo più preoccupante è costituito da finestre che appaiono a caso o di continuo. Alcune di queste finestre hanno l'aspetto di una finestra di dialogo di Windows (messaggio di avviso).

TUO NEMICO

NEWBIE

SOCIAL ENGINEERING

Dove non arrivano i virus, arriva l'uomo. Ecco il social engineering, la versione riveduta e corretta delle truffe nello stile del film La Stangata...

Una tattica di frode informatica molto insidiosa è il cosiddetto social engineering. In pratica il truffatore che ha bisogno di nostri dati personali come una password, la nostra data di nascita o il nostro numero di conto corrente invece di perdere tempo a cercare di ottenerli dal nostro sistema va direttamente alla sorgente... li chiede a noi. Può sembrare assurdo ma purtroppo funziona molto bene. Il truffatore infatti userà un pretesto apparentemente più che credibile per ottenere le informazioni che gli servono. Mettiamo per esempio che voglia ottenere il nostro nome utente e password per accedere a nostro nome a un certo sito. Prima di tutto si creerà un account di e-mail che non desti sospetti. Ci sono siti che permettono di creare account virtuali con il nome che si preferisce. Per esempio se l'indirizzo di posta elettronica del nostro hacker è peppinoomeccanico@hotmail.com difficilmente potremo credere che la mail che ci spedisce arrivi dall'assistenza tecnica della nostra banca. L'hacker potrà per crearsi l'account assistenza@bancasicura.it e far ridirezionare sul suo indirizzo tutti i messaggi inviati a questo account fasullo. Fatto questo, ci manderà una mail del tipo

Gentile Utente,
per offrirLe un miglior sicurezza e protezione dalle frodi abbiamo aggiornato il server software del ns. Internet Provider. Se desidera accedere gratuitamente al nostro programma di sicurezza avanzato La preghiamo di volerci comunicare al più presto il suo username e la sua password, scrivendo al nostro indirizzo email: assistenza@bancasicura.it

Ringraziandola per la cortese attenzione la salutiamo cordialmente
Assistenza Clienti Bancasicura

La lettera sarà probabilmente anche firmata e ci sarà un numero di telefono per ulteriori informazioni. Se non saremo abbastanza ingenui da rispondere alla mail inserendo il nostro nome utente e password e chiameremo il numero in calce... risponderà il nostro truffatore o un suo complice con un professionalissimo "Qui Bancasicura, posso esserle utile?" e noi daremo i nostri dati a lui. Chi pratica il social engineering è infatti abituato a usare non solo la mail ma anche il telefono.

Per esempio, potrebbe chiamarci fingendosi del servizio clienti di qualche nota società di telemarketing e chiederci la data del nostro compleanno perché siamo stati scelti per ricevere un omaggio. L'informazione sembra innocua e glie la diamo, fornendogli un'arma importante per spacciarsi per noi al telefono con la nostra banca o il gestore della nostra carta di credito. La tattica di promettere omaggi, spesso abbastanza modesti da essere credibili, è una delle più usate da chi cerca di ottenere fraudolentamente informazioni via mail o telefono. Dove non arrivano le promesse, d'altra parte, può arrivare un tono autoritario e deciso. Per esempio siamo impiegati di una grande azienda e riceviamo alla nostra scrivania la telefonata di una persona che dice di lavorare per la società che sta aggiornando la rete informatica degli uffici in cui lavoriamo. Quando ci chiede la nostra password siamo titubanti nel dargliela perché ci sembra poco sicuro. Il "tecnico" ci risponde con tono leggermente spazientito che lui è più che felice di andarsi a prendere un caffè invece di finire il lavoro ma che dovrà riferire al Dott. Pistacci (il capo del nostro capo) che siamo stati noi a causare il ritardo. Ecco che la tentazione di fornire il dato si fa più tangibile anche se sappiamo che non sarebbe difficile per un malintenzionato conoscere l'organigramma della nostra azienda.

